# EXHIBIT A

**REESE RICHMAN LLP**
Kim E. Richman
krichman@reeserichman.com
Michael R. Reese
mreese@reeserichman.com
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643-0500
Facsimile: (212) 253-4272

- and -

**MILBERG LLP**
Sanford P. Dumain
sdumain@milberg.com
Peter E. Seidman
pseidman@milberg.com
One Penn Plaza
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

*Attorneys for Plaintiffs and the Proposed Class*

**UNITED STATES DISTRICT COURT**

**EASTERN DISTRICT OF NEW YORK**

| | |
|---|---|
| MICHAEL FROHBERG and ANDY WU, on behalf of themselves and all others similarly situated,<br>Plaintiffs,<br>vs.<br>MEDIA INNOVATION GROUP, LLC and WPP PLC,<br>Defendants. | Case No. ________________<br>**CLASS ACTION COMPLAINT**<br>**DEMAND FOR JURY TRIAL** |

Michael Frohberg and Andy Wu (collectively, "Plaintiffs") allege the following, based upon personal knowledge and upon information and belief derived from, among other things, investigation of counsel and review of public documents.

## NATURE OF THE ACTION

1. This is a class action against Media Innovation Group, LLC ("MIG") and WPP plc ("WPP") (collectively, "Defendants") arising from Defendants' hacking of computers and mobile devices, Defendants' invasion of Internet users' online privacy, and MIG's intentional misrepresentations related to both of these activities.

2. Defendants circumvented the privacy protections on Plaintiffs' Safari[1] web browsers, thereby hacking into Plaintiffs' computers and mobile devices (collectively, "Devices"). Subsequently, Defendants placed cookies on Plaintiffs' Safari browsers that Defendants used to obtain information about Plaintiffs and their Devices as they used Safari to browse web pages to which Defendants delivered web content as a third party. Included in the private information that Defendants obtained in this manner was sensitive, personal, and personally identifiable information, and, as set forth herein, Defendants, without Plaintiffs' knowledge, misappropriated and exploited this private information for their own uses. MIG thereby violated its own privacy policy – *i.e.*, a policy that proudly proclaims MIG's commitment to "protecting the privacy of Internet users." MIG further assured Internet users that adjusting Safari's privacy controls to disallow setting of cookies is an effective way to prevent MIG from collecting information about them as they browse the Internet using Safari. *See* http://www.themig.com/en-us/privacy.html (Under the heading "Information We Collect Through Our [Third Party Advertising] Services", MIG states that "[a]t all times, you may adjust your computer's web browser settings to refuse all cookies.").

3. These actions of Defendants violated New York General Business Law § 349; California Penal Code § 502; Article I, Section 1, of the California Constitution; and California

[1] All references to "Safari" are to the Safari web browser developed by Apple Inc.

Penal Code § 630 *et seq*. Defendants' conduct also constitutes trespass to personal property / chattels under New York common law, invasion of privacy under California common law, and intentional misrepresentation under New York and California common law.

## JURISDICTION AND VENUE

4. This Court has original jurisdiction over this class action under 28 U.S.C. § 1332(d), which, under the provisions of the Class Action Fairness Act ("CAFA"), explicitly provides for the original jurisdiction of the Federal Courts in any class action in which at least 100 members are in the proposed plaintiff class, any member of the plaintiff class is a citizen of a State different from any defendant, and the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs. Plaintiffs allege that the total claims of individual members of the proposed Class are well in excess of $5,000,000 in the aggregate, exclusive of interest and costs.

5. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391. Substantial acts in furtherance of the alleged improper conduct, including hacking of Plaintiffs' and the Class members' Devices, occurred within this District.

## THE PARTIES

6. Plaintiff Michael Frohberg resides in New York and uses his Device there. Mr. Frohberg values his online privacy, especially when using the Internet in the seclusion of his home and/or when conducting his personal affairs. Mr. Frohberg browses the Internet using the Safari browser on his computer. At all relevant times, Safari's "Third-Party-Blocking Only Option" (described in detail below) was either operating by default or had been selected by Mr. Frohberg. Mr. Frohberg used Safari to visit web pages that included advertisements (the "Hacking Ads", described in detail below) that Defendants used to hack into his Device and, subsequently, to place tracking mechanisms called "cookies" on the Device. Defendants used the cookies so placed (in the case of MIG, a cookie called "id", and in the case of WPP, a cookie called "OAX") to obtain "End User Information" (as defined below) about Mr. Frohberg and his Device as he used Safari to browse web pages to which Defendants delivered web content. In

this manner, Defendants obtained private information about Mr. Frohberg and his Device without his permission and against his will (as expressed by means of Safari's Third-Party-Blocking Only Option). Mr. Frohberg mistakenly believed that Safari's privacy controls protected him from having his information obtained by Defendants (in the manner described herein), and Mr. Frohberg mistakenly believed that Defendants' Hacking Ads were a benign part of the online environment. When Mr. Frohberg discovered that Defendants had hacked his Device and learned and collected private information about him without his permission, Mr. Frohberg was shocked, humiliated, and angered and he suffered emotional distress. Furthermore, Defendants' conduct undermined Mr. Frohberg's faith and confidence in the trustworthiness and integrity of the Internet. Defendants degraded the value of Mr. Frohberg's Device and deprived him of the ability to sell to Defendants the information that Defendants collected against his will.

7. Plaintiff Andy Wu resides in California and uses his Devices there. Mr. Wu values his online privacy, especially when using the Internet in the seclusion of his home and/or when conducting his personal affairs. Mr. Wu browses the Internet using the Safari browser on both his iPad and computer. At all relevant times, Safari's Third-Party-Blocking Only Option was either operating by default or had been selected by Mr. Wu. Mr. Wu used Safari to visit web pages that included Hacking Ads that Defendants used to hack into his Devices and, subsequently, to place the "id" and "OAX" cookies on the Devices. Defendants used the cookies to obtain End User Information about Mr. Wu and his Devices as he used Safari to browse web pages to which Defendants delivered web content. In this manner, Defendants obtained private information about Mr. Wu and his Devices without his permission and against his will (as expressed by means of Safari's Third-Party-Blocking Only Option). Mr. Wu mistakenly believed that Safari's privacy controls protected him from having his information obtained by Defendants (in the manner described herein), and Mr. Wu mistakenly believed that Defendants' Hacking Ads were a benign part of the online environment. When Mr. Wu discovered that Defendants had hacked his Devices and learned and collected private information about him without his permission, Mr. Wu was shocked, humiliated, and angered and he suffered emotional

distress. Furthermore, Defendants' conduct undermined Mr. Wu's faith and confidence in the trustworthiness and integrity of the Internet. Defendants degraded the value of Mr. Wu's Devices and deprived him of the ability to sell to Defendants the information that Defendants collected against his will. (Exhibit 1 hereto shows the results of a diagnostic test performed on Mr. Wu's iPad through the website of the Network Advertising Initiative, a self-regulatory organization comprised of over 80 online advertising companies, including MIG.).

8. Defendant Media Innovation Group, LLC is an advertising technology provider within the WPP family of companies. MIG is a Delaware limited liability company that maintains its corporate headquarters at 132 West 31st Street, 12th Floor, New York, New York 10001. *See* http://www.wpp.com/wpp/companies/officedetail.htm?id=6212. MIG conducts business throughout New York, the nation, and internationally.

9. Defendant WPP plc is a public limited company that maintains its principal executive office in Dublin, Ireland, and its main management office in London, United Kingdom. WPP has an office in New York, New York, and owns MIG. WPP is a foreign private issuer registered with the Securities and Exchange Commission as WPP plc, and is traded on the NASDAQ as WPPGY. WPP conducts business throughout New York, the nation, and internationally.

## STATEMENT OF THE CASE

10. People have incorporated the web into their personal lives, through the use of things like social media, dating sites, digital commerce, political forums, and sites containing medical information. *See* The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (2012) (Foreword).

11. Plaintiffs at all relevant times used the Internet to communicate with others via social media, to engage in commerce, and to search for a wide variety of information, much of it personal, sensitive, and private. They often browsed the Internet from the seclusion of their homes and at all relevant times did not expect, nor did they have any reason to expect, that outsiders would observe or record their online activities.

12. This expectation derived, in part, from various mechanisms that are designed to grant Plaintiffs control over who may access information about them and their Devices as they browse the Internet.[2] These mechanisms include the privacy controls incorporated into Apple Inc.'s Safari web browser (the "Privacy Controls").[3] Safari's Privacy Controls are adjustable at the discretion of the Safari user. At all relevant times, Plaintiffs had available a choice:

(a) They could keep their "End User Information" (as defined below) secret from all websites.

(b) They could keep their End User Information secret from all websites except for the websites whose web pages they visited (the "First Party Content Providers"). For example, if a Safari user chose this option and then visited a web page on the site located at http://www.amazon.com/ ("amazon.com"), Safari would allow amazon.com to set cookies on the Safari user's Device.[4] If amazon.com then set a cookie(s) on the user's Device, amazon.com could use the cookie(s), among other things, to facilitate collection of End User Information about the Safari user whenever the user visited web pages that included content provided by amazon.com, [5] to streamline the purchase process, or to facilitate

[2] The "Do Not Track" system, which allows consumers to signal to online companies that they do not want to be tracked, is one such mechanism. *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* i, iii, v (Mar. 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[3] The Privacy Controls only protect Internet users when they are browsing using Safari. The Privacy Controls have no effect on and cannot protect browsing conducted using other web browsers, such as Windows Internet Explorer (developed by Microsoft Corporation) or Mozilla Firefox (developed by Mozilla Foundation and Mozilla Corporation).

[4] In this instance, amazon.com is the website acting as the First Party Content Provider.

[5] Practically speaking, a website cannot efficiently and reliably collect End User Information about an Internet user without setting a cookie on the Internet user's Device.

recommendation of products based on the user's amazon.com browsing and purchase history. Many Internet users are willing to allow First Party Content Providers to set cookies (and thereby potentially to obtain End User Information about them) because many web pages cannot function properly (or in some cases, at all) if the First Party Content Provider cannot set cookies. This option is the default option in Safari's Privacy Controls – *i.e.*, it is the one that is operational by default and remains in operation unless the Safari user switches to another option. Herein, this option is referred to as the "Third-Party-Blocking Only Option."

(c) They could allow not only First Party Content Providers but also "Third Party Content Providers" to set cookies on their Devices and thereby potentially obtain End User Information about them as they browse the web using Safari. A "Third Party Content Provider" is a website that delivers content to a web page that is part of a separate, different website, as an Internet user is visiting the page.[6] For example, when an Internet user is visiting a web page on the site located at http://www.facebook.com/ ("facebook.com"), the web page may include content (for example, an ad) delivered from the site located at http://www.third-party-advertiser.com/ ("third-party-advertiser.com"). In this instance, facebook.com is acting as a First Party Content Provider and third-party-advertiser.com is acting as a Third Party Content Provider. Herein, the content delivered by a Third Party Content Provider to a First Party Content Provider's web page is called "Third Party Content."[7]

[6] The latter website is thus acting as a First Party Content Provider.

[7] Examples of Third Party Content include advertisements and "web beacons" (further explained herein).

13. A Safari user who has selected the Third-Party-Blocking Only Option can stop the Privacy Controls from keeping End User Information secret from a specific Third Party Content Provider by submitting an online form to that Third Party Content Provider (the "Form Exception").

14. As used herein, the term "End User Information" means information that a website can obtain about an Internet user after the site has set a cookie on the user's Device. The information may be obtained when the user visits either (i) a web page that is part of the site or (ii) a web page to which the site is delivering Third Party Content. End User Information includes but is not limited to the Uniform Resource Locator ("URL") of the page that the user visited (i) on the site or (ii) to which the site delivered Third Party Content; the time at which the user visited the page; details about the operating system on which the user's browser was running (for example, "Mac OS X" on an iPad); and details about the user's web browser (including information about extensions added to the browser). If a site sets a cookie on an Internet user's Device and the user subsequently visits a series of web pages that (i) are part of the site or (ii) are pages to which the site delivers Third Party Content, then the site can collect a list or a history of information about the user (including the information listed in this paragraph).

15. A website can thus collect End User Information about an Internet user when it provides Third Party Content to other sites throughout the web that the user visits, so long as the website has set a cookie on the user's browser. As noted in footnote 7, *supra*, Third Party Content includes but is not limited to ads and "web beacons." "Web beacons" are pieces of web content that are invisible (or extremely small).[8] When a website delivers a web beacon to a web page as Third Party Content, the Internet user visiting the page is almost always unaware that the web beacon is included on the page (unlike the case where an ad is delivered to a web page as

[8] Web beacons are alternatively known as "web bugs", "tags", "tracking pixels", "1 x 1 gifs", and "clear gifs". Upon information and belief, MIG's privacy policy refers to web beacons as "pixels." *See* http://themig.com/en-us/privacy.html ("We collect Non-PII through the use of cookies, pixels and related technology.").

Third Party Content). The purpose, however, of delivering a web beacon as Third Party Content to a web page is not for the Internet user visiting the page to see the web beacon. It is instead to allow the site delivering the web beacon to obtain End User Information about the user (which is, practically speaking, only possible when the Third Party Content Provider has set a cookie on the user's Device).

16. Few Internet users are willing to allow websites they have never directly visited to obtain End User Information about them, even if those sites have delivered Third Party Content to (first party) web pages that the users have visited.

17. Defendants' business includes delivering ads as Third Party Content to web pages throughout the World Wide Web on behalf of Defendants' advertiser clients.

18. Defendants' business also includes obtaining End User Information about Internet users as the users browse sites to which Defendants deliver Third Party Content (including ads and web beacons), which is possible when Defendants have set cookies on the Internet users' Devices.

19. Defendants used computer programming language contained in some of the ads they delivered to web pages as Third Party Content (the "Hacking Ads") to disable the protection provided by Safari's Privacy Controls – the Safari users' express preference with regard to setting of cookies on their Devices, including cookies used to obtain End User Information – with respect to Defendants. *See infra* ¶ 12.

20. Specifically, when Defendants delivered a Hacking Ad as Third Party Content to a web page that was loading in a Plaintiff's or Class member's Safari browser, the computer programming language within the Hacking Ad caused the browser to *immediately* send an *invisible* online form back to Defendants, triggering Safari's Form Exception with respect to Defendants (*i.e.*, turning off Safari's privacy protections with respect to Defendants).

21. However, a Safari user is the only appropriate person to fill out and send this type of online form from the user's Device to Defendants, especially when doing so has the effect of

disabling Safari's privacy protections with respect to Defendants. Defendants thus hacked Plaintiffs' and the Class members' Devices by means of the Hacking Ads.

After Defendants had hacked Plaintiffs' and the Class members' Devices, Safari's Privacy Controls no longer prevented Defendants from setting cookies on Plaintiffs and the Class members' Devices, including cookies that Defendants could use in conjunction with Third Party Content (as described above) to obtain End User Information about Plaintiffs and the Class members. Specifically, once Defendants had triggered Safari's Form Exception, Defendants were able to and did place a cookie used by MIG and a cookie used by WPP on the Device that was hacked.

22. The cookie that MIG placed was called "id". Each "id" cookie contains an ID that MIG uses for tracking purposes in its "Zeus Advertising Platform" ("ZAP"). ZAP analytics is a tool that provides Internet user data and analysis that enables third party advertisers to serve ads that are tailored to the Internet user's preferences as revealed, in significant part, through their private Internet browsing history. ZAP provides "a holistic view of site analytics and campaign data for a comprehensive understanding of every individual consumer" and collects and stores "over 13 months of historical user-level data and draws from it to provide complex and robust analysis." *See* http://www.netezza.com/documents/MIG_CaseStudy.pdf (case study on MIG prepared by Netezza Corporation).[9] With ZAP, "MIG is currently tracking the effectiveness of every single advertising element within many live campaigns that reach hundreds of millions of unique users per month…." *See id.*

23. The cookie that WPP placed was called "OAX". Each "OAX" cookie contains an ID that WPP uses for tracking purposes with its "B3" product. "B3" is an "ad optimization product" developed by WPP, GroupM (a WPP subsidiary), MIG, and Compete (a Kanter Media company). *See* http://www.wpp.com/wpp/press/press/default.htm?guid={bcf57ca0-dbc0-4329-8410-2a0c876adea0}. According to WPP's website, B3 is the "the leading agency tool for

[9] Netezza Corporation ("Netezza") designs and markets appliances that house databases, as well as software that analyzes and reports on databases. Netezza technology powers the Zeus Advertising Platform. *See* http://www.netezza.com/documents/MIG_CaseStudy.pdf.

acquiring and optimizing display advertising." *See* http://www.wpp.com/wpp/companies/companydetail.htm?id=565.

24. Stanford researcher Jonathan Mayer first identified Defendants' Hacking Ads. Mr. Mayer's blog describes these findings in detail. *See* http://webpolicy.org/2012/02/17/safari-trackers/. Subsequently, Ashkan Soltani, technology adviser for *The Wall Street Journal*, independently confirmed Mr. Mayer's findings. Mr. Soltani surveyed the top 100 most popular websites as ranked by Quantcast in February 2012.

25. On February 17, 2012, *The Wall Street Journal* published an article describing Mr. Mayer's and Mr. Soltani's findings in detail. *See* Julia Angwin & Jennifer Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, Wall St. J., Feb. 17, 2012, *available at* http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

26. Mr. Mayer discovered Defendants' Hacking Ads on the following sites:
http://www.accuweather.com/
http://www.businessinsider.com/
http://www.guardiannews.com/
http://www.sidereel.com/
http://www.tvguide.com/

27. At all relevant times, Plaintiffs were unaware that Defendants had improperly disabled their Safari privacy protections to allow Defendants to collect and exploit End User Information about them, including their private Internet browsing history.

28. To prevent this, Plaintiffs and the Class members could have deleted the "id" and "OAX" cookies or visited certain websites and opted out of tracking by Defendants. Plaintiffs and the Class members, however, did not know that the "id" and "OAX" cookies were on their Devices or that Defendants were obtaining End User Information about them as they surfed the web. Plaintiffs and the Class members instead believed that Safari's Privacy Controls, which were set to the Third-Party-Blocking Only Option, prevented Third Party Content Providers (including Defendants when they were acting as a Third Party Content Provider) from placing cookies on their Devices and obtaining End User Information about them. Plaintiffs and the

Class members therefore had no reason to locate and delete the "id" and "OAX" cookies or to attempt to discover which websites they could use to opt out of tracking by Defendants.

29. Defendants injured Plaintiffs and the Class members by hacking their Devices.

30. As a result of being hacked, the Devices no longer functioned as they normally should have.

31. By hacking the Devices and impairing their functionality, Defendants degraded their value.

32. Upon discovering that Defendants had hacked their Devices and obtained private End User Information about them without their permission and against their will (as expressed by means of Safari's Third-Party-Blocking Only Option), Plaintiffs and the Class members were shocked, humiliated, and angered, and suffered emotional distress.

33. By the above actions, Defendants undermined Plaintiffs' and the Class members' confidence in the safety and trustworthiness of the digital environment.

**<u>The Value of People's Personal Information</u>**

34. The personal information that Defendants collected is an asset that is priced, bought, and sold in discrete units for marketing and other purposes. "Websites and stores can . . . easily buy and sell information on valued visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them." Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, & Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214. The more information that is known about a consumer, the more a company will pay to deliver a precisely targeted advertisement to him or her. *See* Federal Trade Commission (FTC), Protecting Consumer Privacy in an Era of Rapid Change, Preliminary Staff Report (Dec. 2010) ("FTC Report"), at 24.

35. Personal data is viewed as currency. "In many instances, consumers pay for free content and services by disclosing their personal information," according to former FTC commissioner Pamela Jones Harbour. FTC Roundtable Series 1 on: Exploring Privacy (Matter

No. P095416) (Dec. 7, 2009), at 148, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/ PrivacyRoundtable_Dec 2009_Transcript.pdf. In *Property, Privacy, and Personal Data,* Professor Paul M. Schwartz wrote:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

36. On February 28, 2011, *The Wall Street Journal* highlighted a company called "Allow Ltd.," which is one of nearly a dozen companies that offers to sell people's personal information on their behalf and which gives its users 70% of such sales. *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, Wall St. J., Feb. 28, 2011, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html. For example, one Allow Ltd. user received a payment of $8.95 for letting Allow tell a credit card company the user was shopping for a new credit card. *Id.*

37. On February 15, 2012, *The Financial Times* acknowledged the value of personal information in the Internet age in the context of Facebook, Inc.'s upcoming initial public offering: "Two weeks ago Facebook announced an initial public offering that could value the company at up to $100bn. Facebook is worth so much because of the data it holds on its 845m users."[10]

38. As noted in *The Wall Street Journal*, "[t]rade in personal data has emerged as a driver of the digital economy. Many tech companies offer products for free and get income from online ads that are customized using data about customers. These companies compete for ads, in part, based on the quality of the information they possess about users." Angwin & Valentino-

[10] Richard Falkenrath, *Google Must Remember Our Right to be Forgotten*, Fin. Times, *available at* http://www.ft.com/intl/cms/s/0/476b9a08-572a-11e1-869b-00144feabdc0.html#axzz1mgPiI5Ux.

Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy.*

39. Google Inc. ("Google") also acknowledges the value of web browsing histories by purchasing such histories directly from web users. Google's "Screenwise" panel is a program whereby a few thousand Google users are allowing Google to track their web browsing histories in return for up to $25 in gift cards. *See* http://www.google.com/landing/screenwisepanel/.

40. Defendants ultimately profited from using the information they collected after hacking Plaintiffs' and the Class members' Devices in, among other things, their online advertising business.

41. By the above actions, Defendants deprived Plaintiffs and the Class members of the ability to sell their personal information, including web browsing histories, to Defendants.

**Media Innovation Group, LLC's Intentional Misrepresentations**

42. In its privacy policy, MIG purports to be committed to "protecting the privacy of Internet users" and states that adjusting browser privacy controls to disallow setting of cookies is an effective way to prevent information collection by MIG. *See* http://www.themig.com/en-us/privacy.html (Under the heading "Information We Collect Through Our [Third Party Advertising] Services", MIG states that "[a]t all times, you may adjust your computer's web browser settings to refuse all cookies.").

43. However, contrary to MIG's representations, adjusting Safari's Privacy Controls to the Third-Party-Blocking Only Option is completely ineffective at preventing MIG from setting cookies on a Safari user's Device when MIG delivers a Hacking Ad(s) to a web page visited by the Safari user, as detailed herein.

44. Further, MIG's actions, as detailed herein, undercut its purported commitment to protection of people's privacy as they surf the web.

45. MIG's privacy policy further states that MIG is "committed to observing applicable industry guidelines, including those established by the Network Advertising Initiative [("NAI")] and the Interactive Advertising Bureau [("IAB")]" and that MIG is a member of the

NAI and the Digital Advertising Alliance ("DAA"). *See* http://www.themig.com/en-us/privacy.html.

46. The NAI, the IAB, and the DAA all state publicly that web browser privacy controls are an effective means of blocking the setting of cookies. Further, the NAI and the DAA specifically state that use of Safari's Privacy Controls is an effective means of blocking information collection by Third Party Content Providers. *See* http://www.networkadvertising.org/managing/faqs.asp#question_13 [the NAI website] ("[To prevent third party tracking using Safari,] you may confirm that your browser is set to accept only first party cookies and do nothing. This default setting will block all third-party cookies, including those of our member ad networks and those of other, non-member ad networks"); http://www.iab.net/privacymatters/3.php [the IAB website] (click "Basic Steps" to open a list of "smart precautions") ("You can manage your cookies by going into your browser's privacy settings to accept all cookies, no cookies, or save cookies only from sites you know and trust."); http://www.aboutads.info/consumers#browsers [the DAA website] ("Most modern web browsers contain extensive controls that give you the ability to make choices about your privacy. Among other things these controls enable you to block or limit cookies."; linking to Apple's page detailing Safari's capabilities).

47. In spite of MIG's representation that it observes industry guidelines, MIG's actions, as detailed herein, fly in the face of industry guidelines. While the NAI, the IAB, and the DAA instruct web users that configuring privacy controls to prevent setting of third party cookies is an effective means of preventing third party information collection, and MIG purports to act in accordance with these instructions, MIG does not in reality act in accordance with these instructions, as detailed herein.

## CLASS ACTION ALLEGATIONS

48. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a class of Internet users (collectively, the "Class") defined as follows:

> All Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that disabled their Privacy

> Controls with respect to Defendants, enabling Defendants to place the "id" and "OAX" cookies on the users' Devices, and (3) on whose Devices Defendants then placed the "id" and "OAX" cookies. The class period runs from the date that Defendants first began delivering Hacking Ads to web pages to the date of filing of this complaint (the "Class Period").

49. Plaintiffs also bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a subclass of Internet users residing in New York (collectively, the "New York Subclass") defined as follows:

> All New York Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that disabled their Privacy Controls with respect to Defendants, enabling Defendants to place the "id" and "OAX" cookies on the users' Devices, and (3) on whose Devices Defendants then placed the "id" and "OAX" cookies; during the Class Period.

50. Plaintiffs also bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a subclass of Internet users residing in California (collectively, the "California Subclass") defined as follows:

> All California Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that hacked their Privacy Controls, enabling Defendants to place the "id" and "OAX" cookies on the users' Devices, and (3) on whose Devices Defendants then placed the "id" and "OAX" cookies; during the Class Period.

51. Excluded from the Class are Defendants; any parent, subsidiary, or affiliate of Defendants or any employees, officers, or directors of Defendants; legal representatives, successors, or assigns of Defendants; and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

52. **Numerosity**. The Class members are so numerous and dispersed nationwide that joinder of all members is impracticable. Upon information and belief, there are millions of Internet users whose Safari Privacy Controls have been debilitated by Defendants' Hacking Ads. The exact number of Class members is unknown, but Plaintiffs reasonably estimate and believe that there are millions of persons in the Class.

53. **Commonality**. There are numerous and substantial questions of law and fact that are common to all members of the Class, which predominate over any question affecting only

individual Class members. The members of the Class were and potentially continue to be subjected to the same practices of Defendants. The common questions and issues raised by Plaintiffs' claims include, *inter alia*, the following:

(a) whether Defendants hacked Plaintiffs' and the Class members' Devices using Hacking Ads; and

(b) whether Defendants collected Plaintiffs and the Class members' web browsing histories against their will.

54. **Typicality**. Plaintiffs' claims are typical of the claims of all of the other members of the Class, because their claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendants.

55. **Adequacy**. Plaintiffs will fairly and adequately protect the interests of all members of the Class in the prosecution of this action and in the administration of all matters relating to the claims stated herein. Plaintiffs are similarly situated with, and have suffered similar injuries to, the members of the Class they seek to represent. Plaintiffs have retained counsel experienced in handling class action lawsuits. Neither Plaintiffs nor their counsel have any interest that might cause them not to vigorously pursue this action.

56. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy, since individual joinder of the Class members is impracticable. Even if individual Class members were able to afford individual litigation, it would be unduly burdensome to the Courts in which the individual litigation would proceed. Defendants have subjected the Class to the same violations as referenced herein. Accordingly, class certification is appropriate under Rule 23 because common issues of law and fact regarding Defendants' uniform violations predominate over individual issues, and class certification is a superior method of resolving these claims. No unusual difficulties are likely to be encountered in the management of this action as a class action. Defendants have acted in a manner that affects Plaintiffs and all Class members alike, thereby making appropriate injunctive, declaratory, and other relief appropriate with respect to the Class as a whole.

## CAUSES OFACTION

## COUNT ONE

## (VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349)

57. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

58. New York General Business Law § 349 prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state…."

59. In violation of § 349, Defendants engaged in material, deceptive, consumer-oriented acts in the conduct of business that injured Plaintiffs and the Class members.

60. Specifically, Plaintiffs and the Class members mistakenly believed that viewing web pages that included Hacking Ads would not harm their Devices.

61. Defendants' Hacking Ads appeared to be a non-invasive, benign part of the digital environment.

62. In reality, Defendants used their Hacking Ads to harm Plaintiffs' and the Class members' Devices by debilitating the functionality of their Safari Privacy Controls, as described herein.

63. Further, Plaintiffs and the Class members mistakenly believed that Defendants would respect that they, via Safari's Privacy Controls, had explicitly denied permission to Defendants to use Third Party Content in conjunction with cookies to obtain End User Information about them.

64. In reality, Defendants ignored Plaintiffs' and the Class members' explicit prohibition, disabled the functionality of Safari's Privacy Controls, and used their Third Party Content in conjunction with cookies they set on Plaintiffs' and the Class members' Devices to obtain End User Information about Plaintiffs and the Class members as they visited web pages throughout the web.

65. Defendants' acts and/or omissions were generally aimed at the consuming public.

66. These unlawful deceptive acts directly and proximately caused harm to Plaintiffs and the Class members in the following ways:

(a) through the degradation in value of their Devices;

(b) through the loss of their privacy and the exposure of their personal, sensitive, and private information, as a result of which Plaintiffs and the Class members were shocked, humiliated, and angered and suffered emotional distress;

(c) by depriving Plaintiffs and the Class members of the ability to sell their personal information, including their web browsing histories, to Defendants.

67. As a direct and proximate result of Defendants' violation of § 349, Plaintiffs and the Class members have suffered damages in an amount to be determined at trial.

68. Plaintiffs and the Class members have also suffered irreparable injury as a result of Defendants' unlawful conduct, including the unauthorized collection of their personal information. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class members have no adequate remedy at law, entitling them to injunctive relief.

## COUNT TWO

## (VIOLATION OF THE CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CALIFORNIA PENAL CODE § 502)

69. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

70. California Penal Code § 502(c)(1) prohibits a person from knowingly accessing and without permission altering, damaging, and/or otherwise using data, computers, computer systems, and/or computer networks to:

(A) execute a scheme or artifice to defraud or deceive, and/or

(B) wrongfully control or obtain money, property, or data.

71. In violation of § 502(c)(1), Defendants intentionally and without permission altered, damaged, and otherwise used Plaintiffs' and the Class members' Devices to execute a scheme or artifice to defraud or deceive.

72. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Devices as part of the execution of a scheme in which Defendants intentionally failed to inform Plaintiffs and the Class members that Defendants had hacked their Devices and subsequently used Third Party Content in conjunction with cookies to End User Information about Plaintiffs and the Class members as they surfed the web.

73. In violation of § 502(c)(1), Defendants intentionally and without permission altered, damaged, and otherwise used Plaintiffs' and the Class members' Devices to wrongfully control or obtain money, property, or data.

74. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Devices without their knowledge to obtain personal data about them, including their web browsing histories. Further, the personal data that Defendants obtained is property.

75. California Penal Code § 502(c)(2) prohibits a person from knowingly accessing and without permission taking, copying, and/or making use of data from a computer, computer system, and/or computer network.

76. In violation of § 502(c)(2), Defendants intentionally and without permission took, copied, and/or made use of data from Plaintiffs' and the Class members' Devices.

77. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Devices and took information about their web surfing from the Devices, which Defendants made use of in their advertising business.

78. California Penal Code § 502(c)(3) prohibits a person from knowingly and without permission using "computer services" as that term is defined in California Penal Code § 502(b)(4).

79. In violation of § 502(c)(3), Defendants intentionally and without permission used "computer services," including but not limited to storage functions and web history tracking.

80. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Devices, stored cookies on the Devices, and used those cookies in conjunction with browser software on the Devices to obtain End User Information about Plaintiffs and the Class members as they browsed web pages to which Defendants delivered Third Party Content.

81. California Penal Code § 502(c)(4) prohibits a person from knowingly and without permission adding, altering, and/or damaging data, computer software, and/or computer programs that reside and/or exist internal and/or external to a computer, computer system, and/or computer network.

82. In violation of § 502(c)(4), Defendants intentionally and without permission added, altered, and/or damaged data, computer software, and/or computer programs that resided internal to Plaintiffs' and the Class members' Devices.

83. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Safari Privacy Controls, debilitating their functionality.

84. Further, Defendants intentionally and without permission added cookies to Plaintiffs' and the Class members' Devices.

85. California Penal Code § 502(c)(5) prohibits a person from knowingly and without permission disrupting and/or causing the disruption of "computer services" (as that term is defined in California Penal Code § 502(b)(4)) to an authorized user of a computer, computer system, and/or computer network.

86. In violation of § 502(c)(5), as described in detail herein, Defendants disabled the functionality of Plaintiffs' and the Class members' Safari Privacy Controls, thereby disrupting Plaintiffs' and the Class members' desired use of their web browsers and the World Wide Web.

87. California Penal Code § 502(c)(7) prohibits a person from knowingly and without permission accessing computers, computer systems, and/or computer networks.

88. In violation of § 502(c)(7), as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Safari Privacy Controls and placed cookies on their Devices,

which Defendants used in conjunction with Third Party Content to obtain End User Information about them as they surfed the web.

89. California Penal Code § 502(c)(8) prohibits a person from knowingly introducing "computer contaminants" – as defined in California Penal Code § 502(b)(10) – into computers, computer systems, and/or computer networks.

90. In violation of § 502(c)(8), as described in detail herein, Defendants intentionally introduced computer programming code into Plaintiffs' and the Class members' Devices that "usurp[ed] the normal operation" of the Devices by hacking Safari's Privacy Controls, enabling the placement of cookies on the Devices.

91. As a direct and proximate result of Defendants' violation of California Penal Code § 502, Defendants caused loss to Plaintiffs and the Class members in an amount to be proven at trial.

92. Plaintiffs and the Class members are entitled to recovery of attorneys' fees pursuant to § 502(e).

93. Plaintiffs and the Class members are entitled to punitive or exemplary damages under California Penal Code § 502(e)(4) because Defendants willfully violated § 502(c) and are guilty of "fraud" as defined by California Civil Code § 3294(c)(3).

94. Under § 3294(c)(3), "fraud" means an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury.

95. As described in detail herein, Defendants intentionally concealed from Plaintiffs and the Class members the fact that Defendants dismantled the privacy safeguards established by their Privacy Controls.

96. As a result of concealing this fact, Defendants intended to and did deprive Plaintiffs and the Class members of their legal right to privacy.

97. Further, as a result of concealing this fact, Defendants intended to profit and did profit by obtaining without authorization personal, private, and sensitive information about

Plaintiffs and the Class members as they surfed the web and using the information in connection with Defendants' advertising business. Defendants' actions deprived Plaintiffs and the Class of the opportunity to sell the information to Defendants. Defendants thereby deprived Plaintiffs and the Class members of valuable property.

98. Plaintiffs and the Class members have also suffered irreparable injury as a result of Defendants' unlawful conduct, including the unauthorized collection of their personal information. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class members have no adequate remedy at law, entitling them to injunctive relief.

## COUNT THREE

## (VIOLATION OF ARTICLE I, SECTION 1 OF THE CALIFORNIA CONSTITUTION)

99. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

100. Article I, Section 1 of the California Constitution states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

101. Plaintiffs and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their Devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy controls.

102. Plaintiffs and the Class members have a legally protected privacy interest in the End User Information (including personal, confidential, and sensitive information and web browsing histories) that Defendants obtained by hacking Plaintiffs' and the Class members' Safari Privacy Controls.

103. Plaintiffs and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their Devices free of interference, including decisions related to web browser privacy controls.

104. Plaintiffs and the Class members reasonably expected that their End User Information (including personal, confidential, and sensitive information) and intimate personal decisions would be kept private.

105. Defendants committed a serious invasion of Plaintiffs' and the Class members' privacy interests by hacking their Safari Privacy Controls. Unbeknownst to Plaintiffs and Class members, Defendants made a private decision on behalf of Plaintiffs and the Class members that Defendants were not authorized to make.

106. Defendants committed a serious invasion of Plaintiffs' and the Class members' privacy interests by, after hacking their Safari Privacy Controls, obtaining End User Information (including personal, confidential, and sensitive information) about them as they surfed the web without authorization.

107. By the acts, transactions, and courses of conduct alleged herein, Defendants violated Plaintiffs' and the Class members' inalienable right to privacy.

108. As a consequence, Plaintiffs and the Class members were personally injured and suffered emotional distress damages.

## COUNT FOUR

## (VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT, CALIFORNIA PENAL CODE § 630 *ET SEQ.*)

109. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

110. In violation of California Penal Code § 631, Defendants, by means of a contrivance (or in "any other manner") made an unauthorized connection, electrically or "otherwise", with the wires, lines, cables, or instruments within the State of California over

which communications or messages traveled between Plaintiffs' and the Class members' web browsers and the websites whose web pages they visited.

111. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Safari Privacy Controls, which enabled them to place cookies on Plaintiffs' and the Class members' devices that they were explicitly not authorized to place. The cookies so placed, when used in conjunction with delivery of Third Party Content to Plaintiffs and the Class members (as described above), enabled Defendants to obtain End User Information about Plaintiffs and the Class members that Defendants would not otherwise have been able to obtain. Accordingly, Defendants created an unauthorized connection to Plaintiffs' and the Class members' communications with the websites whose web pages they visited, which occurred over wires, lines, cables, or instruments within the State of California.

112. In violation of California Penal Code § 631, Defendants willfully, intentionally, without the consent of Plaintiffs and the Class members, and in an unauthorized manner, obtained, read, attempted to read, learned, and/or attempted to learn the contents of Plaintiffs' and the Class members' electronic communications with (or messages to) the websites whose web pages they visited while the communications (or messages) were in transit in or through California and/or while they were being sent from or received at a place within California.

113. Further, websites whose web pages were visited by Plaintiffs and the Class members did not have the authority to consent to alteration by Defendants of Plaintiffs' and the Class members' Safari Privacy Controls.

114. Defendants used and communicated such illegally obtained electronic communications of Plaintiffs and the Class members, including use and communication in their online advertising business.

115. As a direct and proximate result of the above-described conduct by Defendants, Plaintiffs and all Class members have suffered, and, unless such conduct is enjoined, will continue to suffer, damages in an amount to be proven at trial.

116. Pursuant to California Penal Code § 637.2, Plaintiffs and the Class members are entitled to recover three times their actual and/or statutory damages from Defendants, for the conduct described herein.

117. Defendants' conduct is causing, and unless enjoined will continue to cause, Plaintiffs and the Class members great and irreparable injury that cannot be fully compensated for or measured in money. Plaintiffs and the Class members have no adequate remedy at law and, pursuant to California Penal Code § 637.2(b), are entitled to preliminary and permanent injunctions prohibiting further use and communication of their unlawfully obtained information.

## COUNT FIVE

## (TRESPASS TO PERSONAL PROPERTY / CHATTELS)

118. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

119. The common law of New York prohibits the intentional intermeddling with personal property in possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

120. In violation of New York common law and as detailed more fully herein, Defendants dispossessed Plaintiffs and the Class members from use and/or access to their Devices, or parts of them, without their knowledge or consent. Further, Defendants' acts constituted an intentional interference with the use and enjoyment of the Devices.

121. Without Plaintiffs' and the Class members' knowledge or consent, Defendants knowingly and intentionally accessed their property and caused them injury.

122. Defendants engaged in deception and concealment in order to gain access to Plaintiffs' and the Class members' Devices.

123. Defendants' hacking of Safari's Privacy Controls and subsequent installation of cookies on Plaintiffs' and the Class members' Devices interfered and/or intermeddled with the Devices, including by altering or damaging controls designed to prevent the information

collection effected by Defendants. Such use, interference, and/or intermeddling was without the knowledge or consent of Plaintiffs and the Class members.

124. Defendants' hacking of Plaintiffs' and the Class members' Devices and subsequent placement of cookies on them impaired their condition and value. In particular, these actions debilitated the functionality of Plaintiffs' and the Class members' Safari Privacy Controls.

125. Defendants' trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and the Class members.

126. As a direct and proximate result of Defendants' trespass to chattels, nuisance, interference, and unauthorized access to and intermeddling with Plaintiffs' and the Class members' Devices, Defendants have injured and impaired the condition and value of the Devices as follows:

(a) By consuming the resources of and/or degrading the performance of Plaintiffs' and the Class members' Devices (including space, memory, processing cycles, and Internet connectivity);

(b) By diminishing the use of, value, speed, capacity, and/or capability of Plaintiffs' and the Class members' Devices;

(c) By altering and controlling the functioning of Plaintiffs' and the Class members' Devices;

(d) By devaluing, interfering with, and/or diminishing Plaintiffs' and the Class members' possessory interest in their Devices;

(e) By infringing on Plaintiffs' and the Class members' right to exclude others from their Devices;

(f) By infringing on Plaintiffs' and the Class members' right to determine, as owners of their Devices, which programs should be installed and operated on the Devices, and how programs should be installed and operated on the Devices;

(g) By compromising the integrity, security, and ownership of Plaintiffs' and the Class members' Devices;

(h) By forcing Plaintiffs and the Class members to expend time and resources in order to remove the cookies installed on their Devices without notice or consent.

127. Plaintiffs and the Class members have no adequate remedy at law.

## COUNT SIX

## (INVASION OF PRIVACY IN VIOLATION OF CALIFORNIA COMMON LAW)

128. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

129. Defendants intruded on Plaintiffs' and the Class members' private affairs and seclusion by hacking their Safari Privacy Controls and placing cookies on their Devices – conduct that Defendants engaged in completely outside of their knowledge and against their express will. The cookies enabled Defendants, without authorization, to obtain End User Information about Plaintiffs and the Class members as they surfed the web, as more fully detailed herein.

130. Plaintiffs and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their Devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy controls.

131. Plaintiffs and the Class members have a legally protected privacy interest in the End User Information (including personal, confidential, and sensitive information and web browsing histories) that Defendants obtained by hacking Plaintiffs' and the Class members' Safari Privacy Controls.

132. Plaintiffs and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their Devices free of interference, including decisions related to web browser privacy controls.

133. Plaintiffs and the Class members reasonably expected that their End User Information (including personal, confidential, and sensitive information) and intimate personal decisions would be kept private.

134. Defendants intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by hacking Plaintiffs' and the Class members' Safari Privacy Controls. Unbeknownst to Plaintiffs and the Class members, Defendants made a private decision on behalf of Plaintiffs and the Class members that Defendants were not authorized to make.

135. Defendants intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by, after hacking Plaintiffs' and the Class members' Safari Privacy Controls, obtaining End User Information about them as they surfed the web without authorization.

136. As a consequence, Plaintiffs and the Class members were personally injured and suffered emotional distress damages.

## COUNT SEVEN

## (INTENTIONAL MISREPRESENTATION)

## (AGAINST MEDIA INNOVATION GROUP, LLC, ONLY)

## (NEW YORK SUBCLASS ONLY)

137. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

138. During the Class Period, MIG engaged in fraudulent, misrepresentative, false, and/or deceptive practices.

139. First, MIG represented to Plaintiffs and the New York Subclass members that MIG was "firmly committed to protecting the privacy of Internet users."

140. MIG made the above representation knowing that MIG was in fact invading Plaintiffs' and the New York Subclass members' online privacy by hacking their Safari Privacy Controls, as detailed herein.

141. Second, under the heading "Information We Collect Through Our [Third Party Advertising] Services" in its privacy policy, MIG represented to Plaintiffs and the New York Subclass members that "[a]t all times, you may adjust your computer's web browser settings to refuse all cookies."

142. MIG made the above representation knowing that MIG was in fact delivering Hacking Ads to Plaintiffs and the New York Subclass members as they surfed the web that were specifically designed to and did disable Safari's Third-Party-Blocking Only Option with respect to MIG, allowing MIG to place cookies on Plaintiffs' and the New York Subclass members' Devices, as detailed more fully herein.

143. Third, MIG represented to Plaintiffs and the New York Subclass members that MIG was in compliance with the guidelines of the NAI, the IAB, and the DAA.

144. The websites of the NAI and the DAA explain that Safari's Privacy Controls, when set to block cookies set by websites acting as Third Party Content Providers, are effective at doing so.

145. The IAB's website explains that web browsers' privacy controls, when set to block the setting of cookies, are effective at doing so.

146. While representing that MIG was acting in accord with the policies and representations of the NAI, the IAB, and the DAA, MIG knowingly was delivering Hacking Ads to Plaintiffs and the New York Subclass members as they surfed the web with the specific purpose of disabling Safari's Privacy Controls, setting cookies on their Devices, and obtaining End User Information about them, as detailed herein.

147. These aforementioned frauds, misrepresentations, deceptive, and/or false acts and omissions concerned material facts that were essential to Plaintiffs' and the New York Subclass members' decisions to browse the web using Safari with the Third-Party-Blocking Only Option selected.

148. Plaintiffs and the New York Subclass members would have acted differently had they not been misled, but, instead, had been informed that Safari's Privacy Controls were

ineffective at preventing MIG from setting cookies on their Devices and, using those cookies in conjunction with MIG's Third Party Content, obtaining End User Information about them as they surfed the web.

149. By and through such fraud, deceit, misrepresentations, and/or omissions, MIG intended to induce Plaintiffs and the New York Subclass members to alter their positions to their detriment.

150. Plaintiffs and the New York Subclass members justifiably and reasonably relied on MIG's omissions and misrepresentations, and, as such, were damaged by MIG.

151. As a direct and proximate result of MIG's omissions and misrepresentations, Plaintiffs and the New York Subclass members have suffered damages, including in the following ways:

(a) On discovering that MIG was hacking their Devices so as to intrude upon their seclusion and observe their personal affairs, as detailed herein, Plaintiffs and the New York Subclass members were shocked, humiliated, and angered, and suffered emotional distress; and

(b) MIG's intentional misrepresentations enabled MIG to collect Plaintiffs and the New York Subclass members' End User Information (including private, personal, and sensitive information and Safari web browsing histories), thereby depriving Plaintiffs and the New York Subclass members of the ability to sell their End User Information to MIG.

## COUNT EIGHT
## (INTENTIONAL MISREPRESENTATION)
## (AGAINST MEDIA INNOVATION GROUP, LLC, ONLY)
## (CALIFORNIA SUBCLASS ONLY)

152. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

153. During the Class Period, MIG engaged in fraudulent, misrepresentative, false, and/or deceptive practices.

154. First, MIG represented to Plaintiffs and the California Subclass members that MIG was "firmly committed to protecting the privacy of Internet users."

155. MIG made the above representation knowing that MIG was in fact invading Plaintiffs' and the California Subclass members' online privacy by hacking their Safari Privacy Controls, as detailed herein.

156. Second, under the heading "Information We Collect Through Our [Third Party Advertising] Services" in its privacy policy, MIG represented to Plaintiffs and the California Subclass members that "[a]t all times, you may adjust your computer's web browser settings to refuse all cookies."

157. MIG made the above representation knowing that MIG was in fact delivering Hacking Ads to Plaintiffs and the California Subclass members as they surfed the web that were specifically designed to and did disable Safari's Third-Party-Blocking Only Option with respect to MIG, allowing MIG to place cookies on Plaintiffs' and the California Subclass members' Devices, as detailed more fully herein.

158. Third, MIG represented to Plaintiffs and the California Subclass members that MIG was in compliance with the guidelines of the NAI, the IAB, and the DAA.

159. The websites of the NAI and the DAA explain that Safari's Privacy Controls, when set to block cookies set by websites acting as Third Party Content Providers, are effective at doing so.

160. The IAB's website explains that web browsers' privacy controls, when set to block the setting of cookies, are effective at doing so.

161. While representing that MIG was acting in accord with the policies and representations of the NAI, the IAB, and the DAA, MIG knowingly was delivering Hacking Ads to Plaintiffs and the California Subclass members as they surfed the web with the specific

purpose of disabling Safari's Privacy Controls, setting cookies on their Devices, and obtaining End User Information about them, as detailed herein.

162. These aforementioned frauds, misrepresentations, deceptive, and/or false acts and omissions concerned material facts that were essential to Plaintiffs' and the California Subclass members' decisions to browse the web using Safari with the Third-Party-Blocking Only Option selected.

163. Plaintiffs and the California Subclass members would have acted differently had they not been misled, but, instead, had been informed that Safari's Privacy Controls were ineffective at preventing MIG from setting cookies on their Devices and, using those cookies in conjunction with MIG's Third Party Content, obtaining End User Information about them as they surfed the web.

164. By and through such fraud, deceit, misrepresentations, and/or omissions, MIG intended to induce Plaintiffs and the California Subclass members to alter their positions to their detriment.

165. Plaintiffs and the California Subclass members justifiably and reasonably relied on MIG's omissions and misrepresentations, and, as such, were damaged by MIG.

166. As a direct and proximate result of MIG's omissions and misrepresentations, Plaintiffs and the California Subclass members have suffered damages, including in the following ways:

(a) On discovering that MIG was hacking their Devices so as to intrude upon their seclusion and observe their personal affairs, as detailed herein, Plaintiffs and the California Subclass members were shocked, humiliated, and angered, and suffered emotional distress; and

(b) MIG's intentional misrepresentations enabled MIG to collect Plaintiffs and the California Subclass members' End User Information (including private, personal, and sensitive information and Safari web browsing histories), thereby depriving Plaintiffs and the California Subclass members of the ability to sell their End User Information to MIG.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs and members of the Class seek relief against Defendants as follows:

A. An order certifying that this action is properly brought and may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs be appointed as Class Representatives, and that Plaintiffs' counsel be appointed Class Counsel.

B. Awarding damages as alleged above.

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class members, including, *inter alia*, an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein.

D. Disgorgement of all revenue earned from selling or otherwise using or trading on the private information obtained from Plaintiffs and the Class members as a result of hacking their Devices, as described herein.

E. Awarding Plaintiffs and the Class members their reasonable litigation expenses and attorneys' fees; and

F. Awarding such other and further relief at law or equity as this court may deem just and proper.

## DEMAND FOR JURY TRIAL

Plaintiffs and the Class members hereby demand trial of their claims by jury to the extent authorized by law.

DATED: May 25, 2012

**REESE RICHMAN LLP**

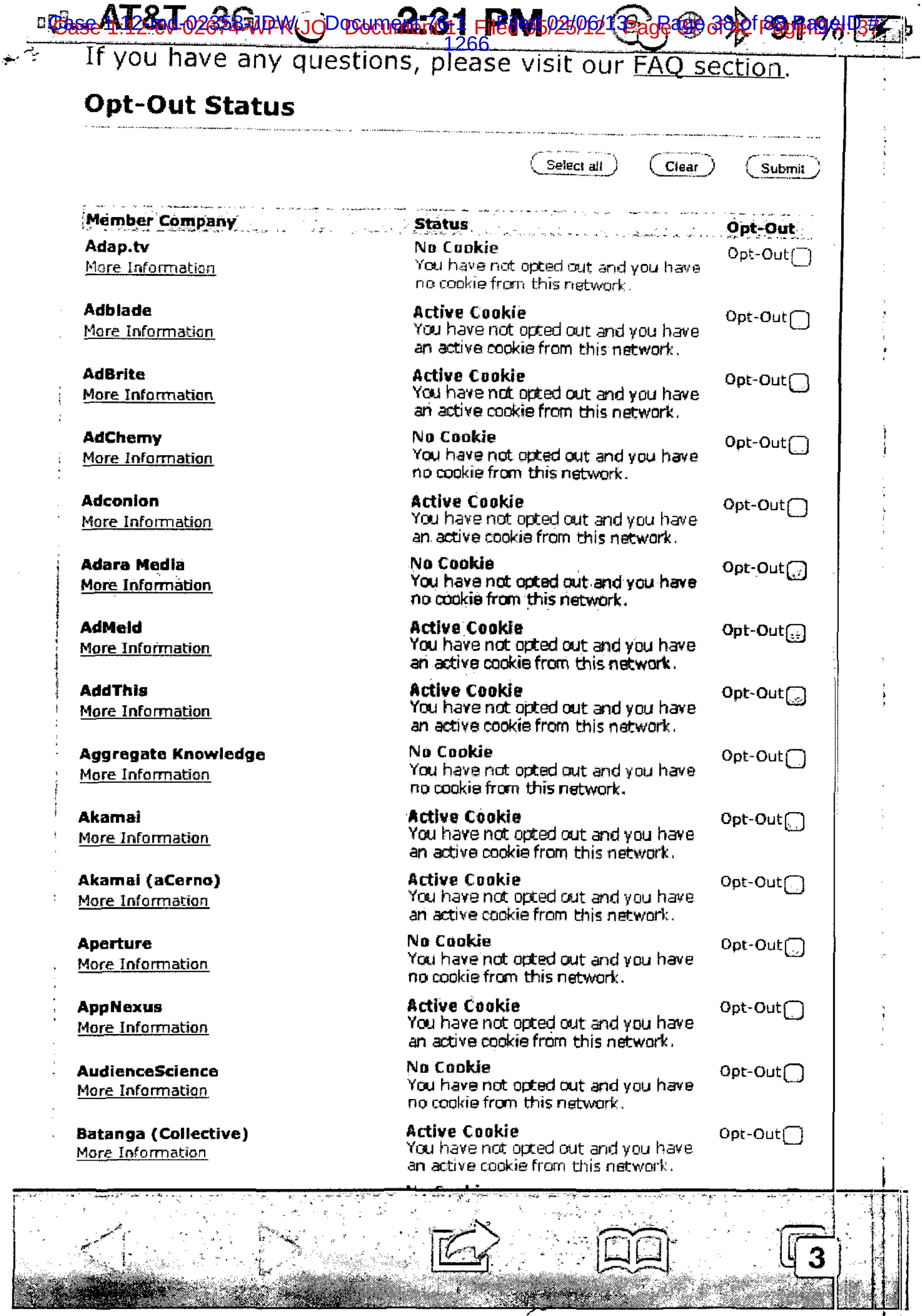
Kim E. Richman
krichman@reeserichman.com
Michael R. Reese
mreese@reeserichman.com
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643-0500
Facsimile: (212) 253-4272

– and –

**MILBERG LLP**
Sanford P. Dumain
sdumain@milberg.com
Peter Seidman
pseidman@milberg.com
One Penn Plaza
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

*Attorneys for Plaintiffs and the Proposed Class*

# EXHIBIT 1

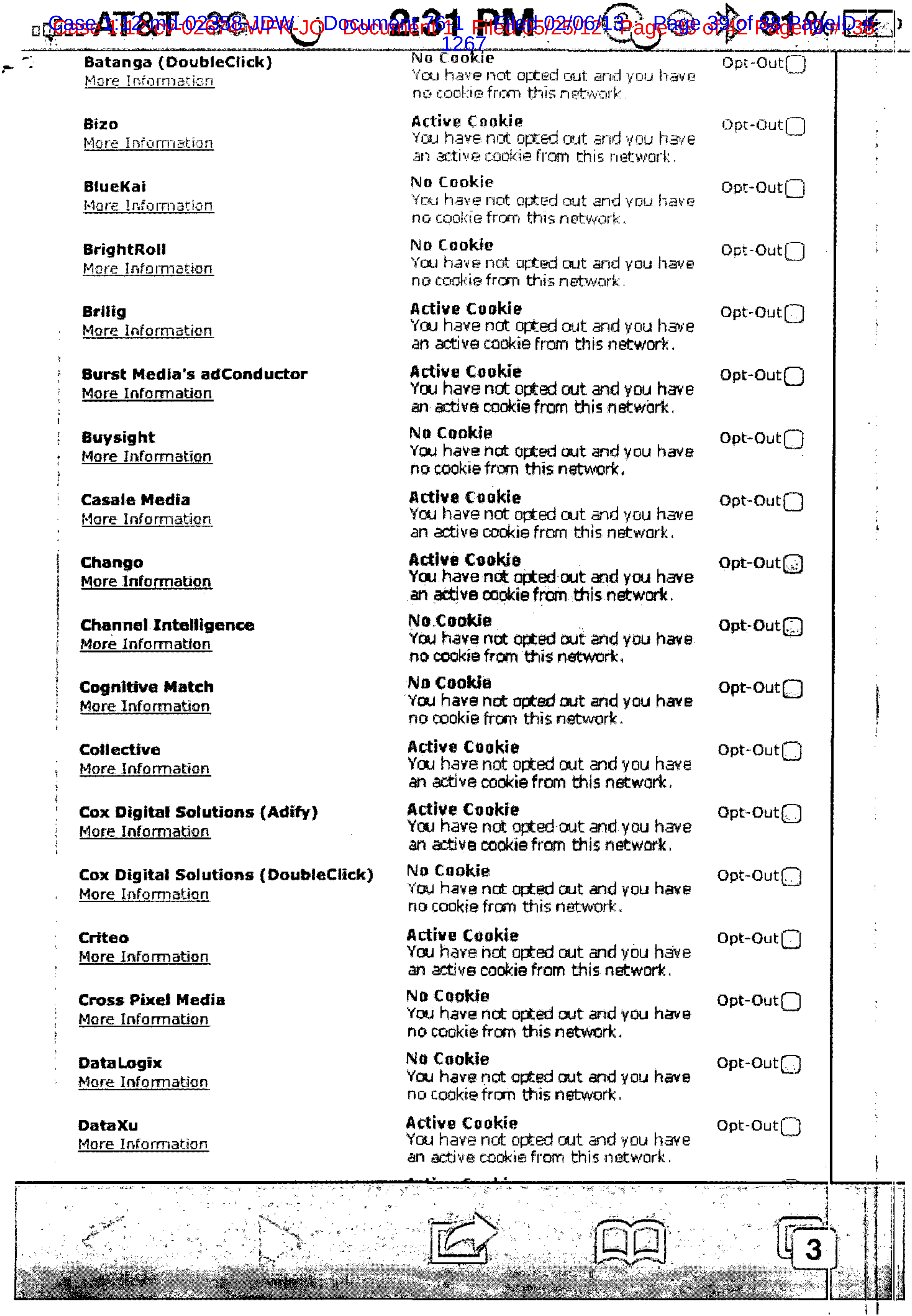


If you have any questions, please visit our FAQ section.

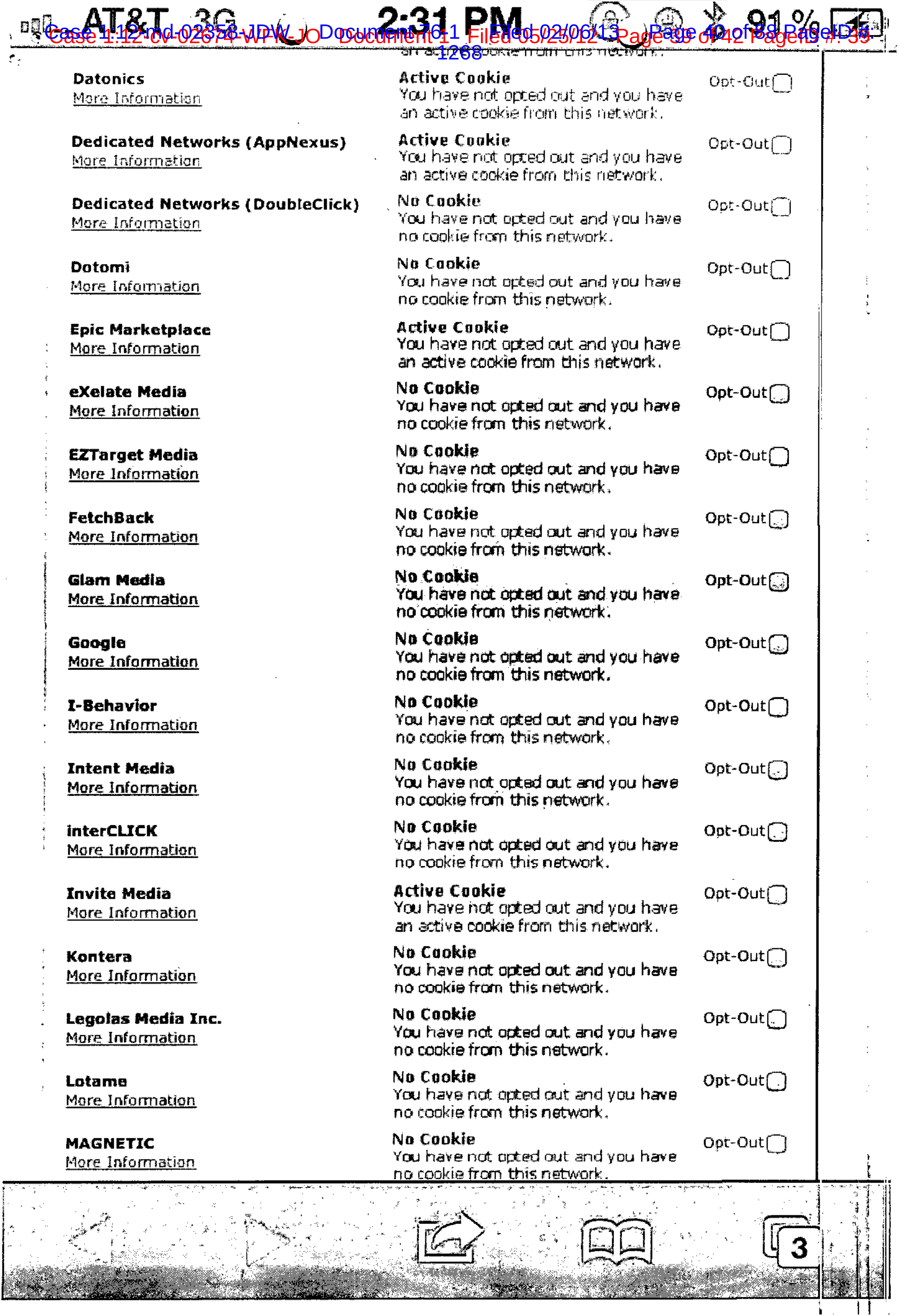
## Opt-Out Status

( Select all ) ( Clear ) ( Submit )

| Member Company | Status | Opt-Out |
|---|---|---|
| **Adap.tv**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Adblade**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **AdBrite**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **AdChemy**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Adconion**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Adara Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **AdMeld**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **AddThis**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Aggregate Knowledge**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Akamai**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Akamai (aCerno)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Aperture**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **AppNexus**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **AudienceScience**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Batanga (Collective)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |

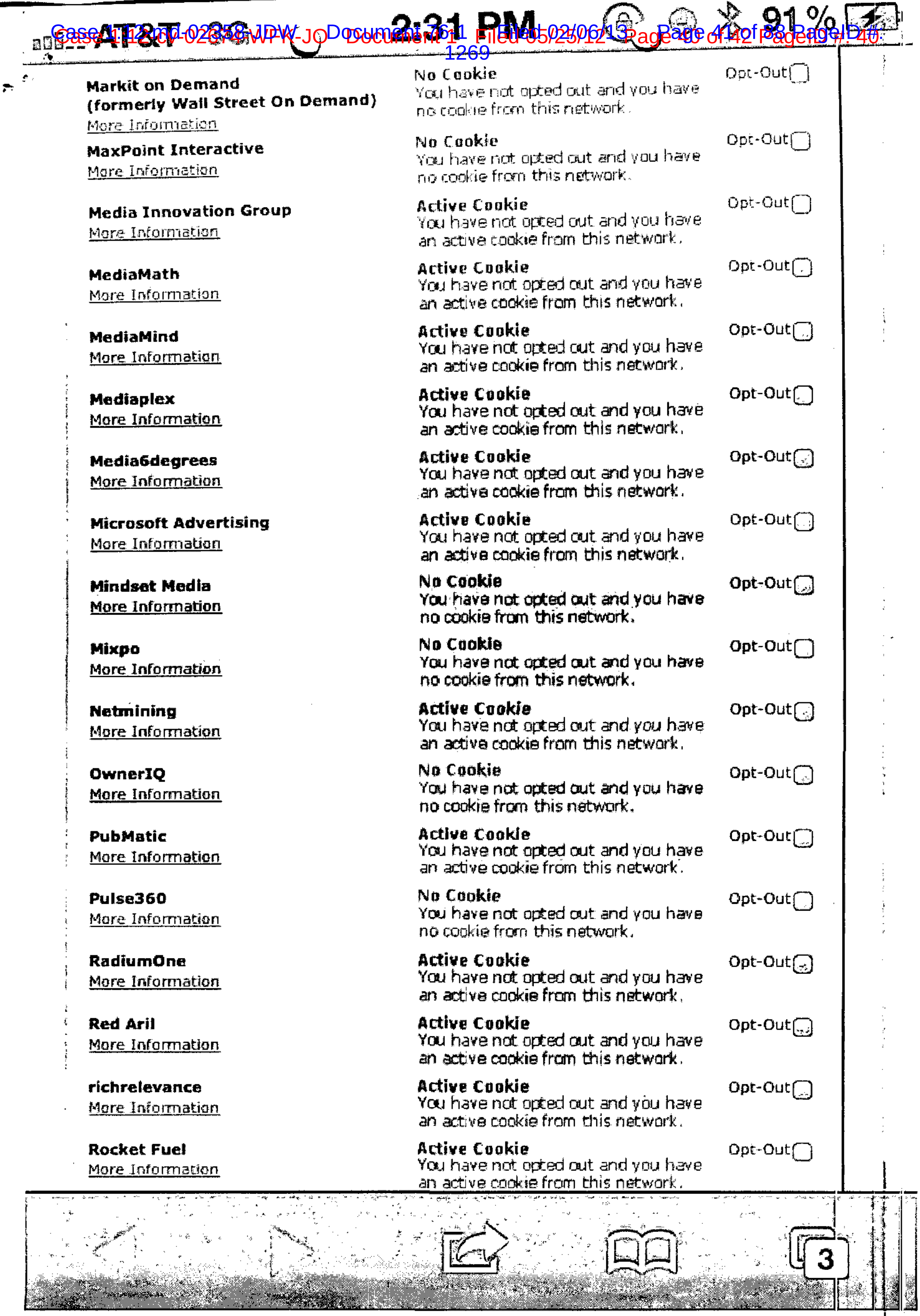


| | | |
|---|---|---|
| **Batanga (DoubleClick)**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Bizo**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **BlueKai**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **BrightRoll**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Brilig**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Burst Media's adConductor**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Buysight**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Casale Media**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Chango**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Channel Intelligence**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Cognitive Match**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Collective**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Cox Digital Solutions (Adify)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Cox Digital Solutions (DoubleClick)**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Criteo**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Cross Pixel Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **DataLogix**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **DataXu**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |

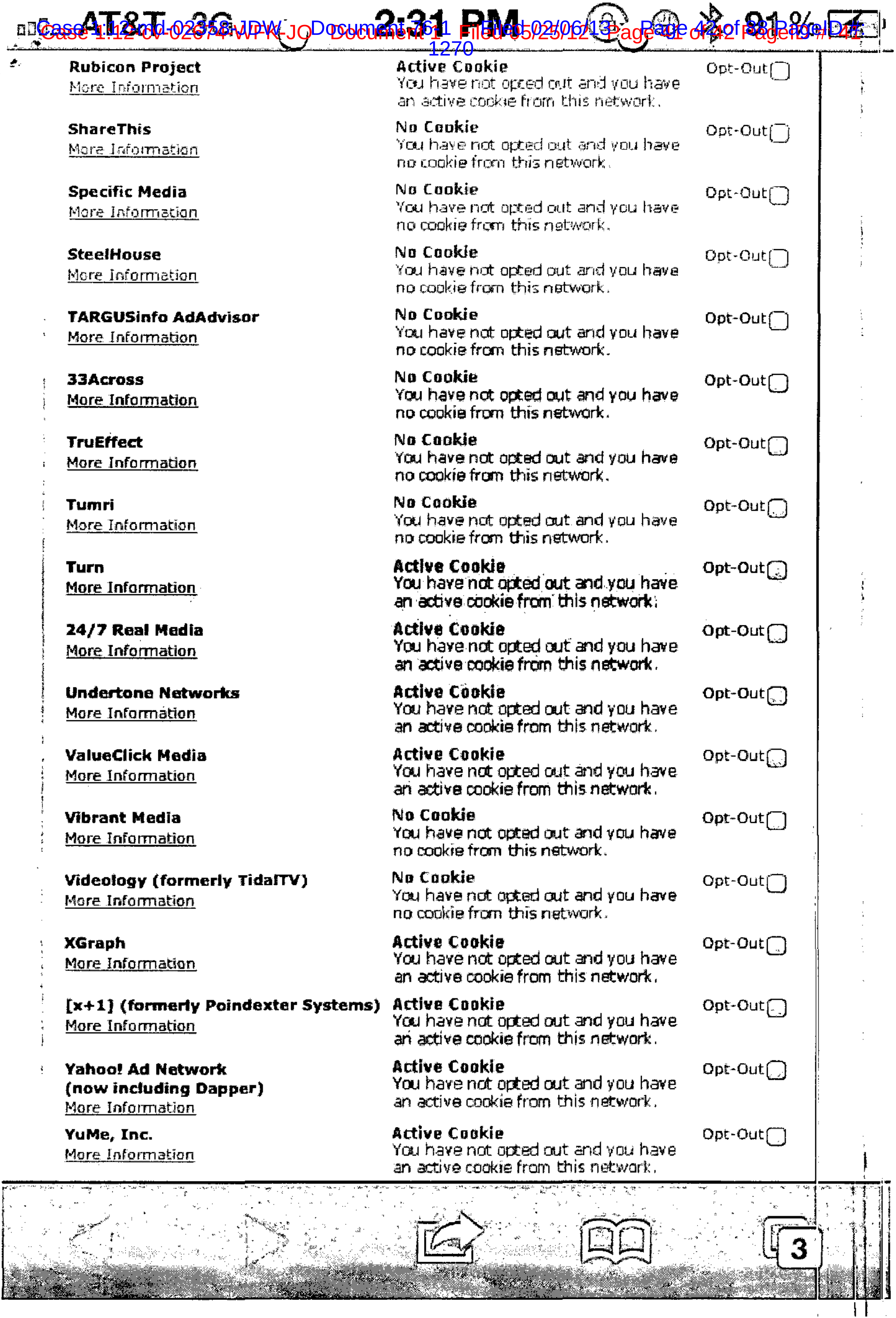


an active cookie from this network.

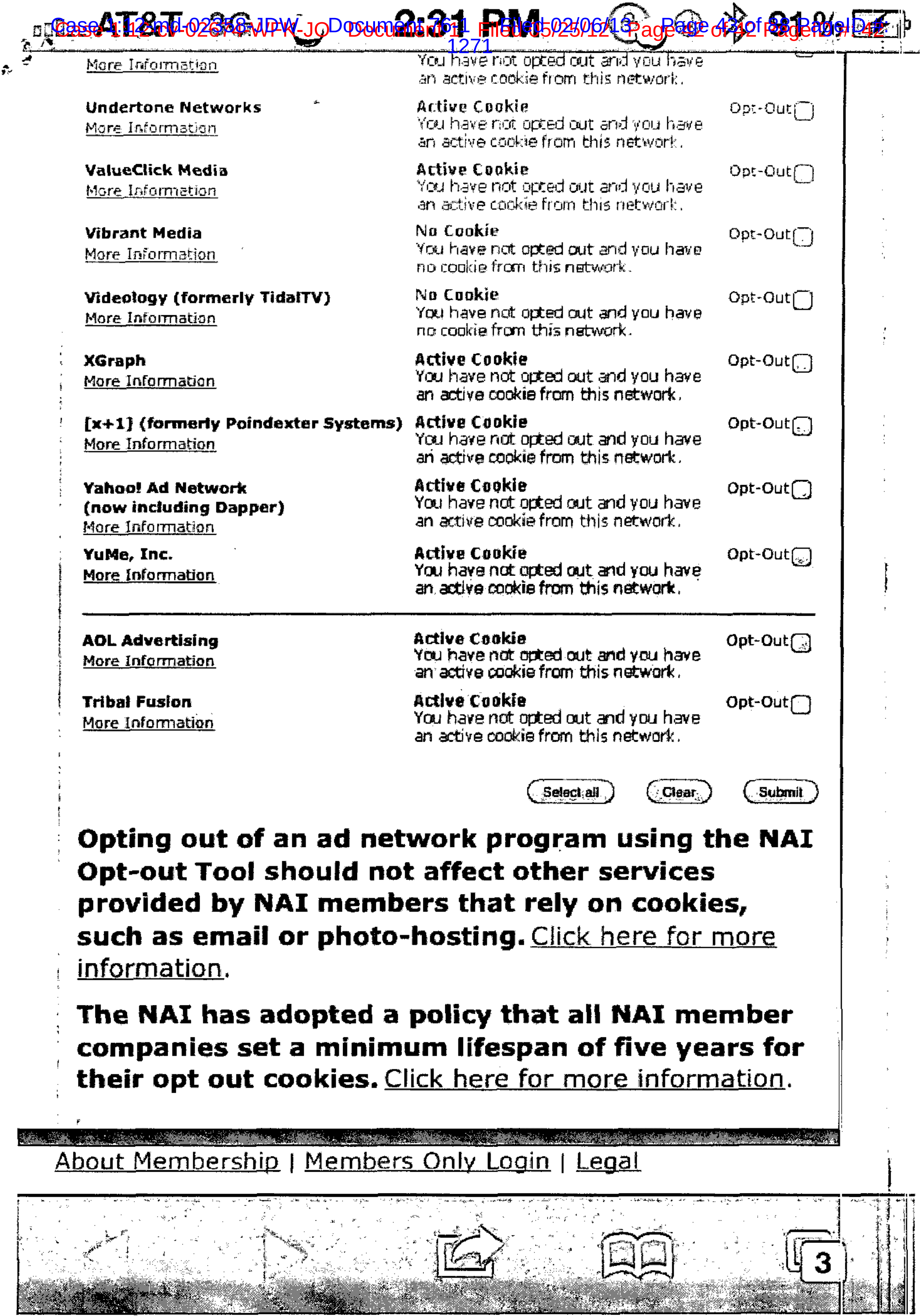
| | | |
|---|---|---|
| **Datonics**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Dedicated Networks (AppNexus)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Dedicated Networks (DoubleClick)**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Dotomi**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Epic Marketplace**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **eXelate Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **EZTarget Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **FetchBack**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Glam Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Google**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **I-Behavior**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Intent Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **interCLICK**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Invite Media**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Kontera**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Legolas Media Inc.**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Lotame**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **MAGNETIC**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |



| | | |
|---|---|---|
| **Markit on Demand (formerly Wall Street On Demand)**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **MaxPoint Interactive**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Media Innovation Group**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **MediaMath**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **MediaMind**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Mediaplex**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Media6degrees**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Microsoft Advertising**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Mindset Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Mixpo**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Netmining**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **OwnerIQ**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **PubMatic**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Pulse360**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **RadiumOne**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Red Aril**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **richrelevance**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Rocket Fuel**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |



| | | |
|---|---|---|
| **Rubicon Project**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **ShareThis**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Specific Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **SteelHouse**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **TARGUSinfo AdAdvisor**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **33Across**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **TruEffect**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Tumri**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Turn**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **24/7 Real Media**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Undertone Networks**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **ValueClick Media**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Vibrant Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Videology (formerly TidalTV)**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **XGraph**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **[x+1] (formerly Poindexter Systems)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Yahoo! Ad Network (now including Dapper)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **YuMe, Inc.**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |



| | | |
|---|---|---|
| More Information | You have not opted out and you have an active cookie from this network. | |
| **Undertone Networks**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **ValueClick Media**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Vibrant Media**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **Videology (formerly TidalTV)**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. | Opt-Out □ |
| **XGraph**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **[x+1] (formerly Poindexter Systems)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Yahoo! Ad Network (now including Dapper)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **YuMe, Inc.**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **AOL Advertising**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |
| **Tribal Fusion**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. | Opt-Out □ |

**Opting out of an ad network program using the NAI Opt-out Tool should not affect other services provided by NAI members that rely on cookies, such as email or photo-hosting.** Click here for more information.

**The NAI has adopted a policy that all NAI member companies set a minimum lifespan of five years for their opt out cookies.** Click here for more information.

About Membership | Members Only Login | Legal

JS 44 (Rev. 09/11)

# CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

**I. (a) PLAINTIFFS**
MICHAEL FROHBERG and ANDY WU, on behalf of themselves and all others similarly situated

**DEFENDANTS**
MEDIA INNOVATION GROUP, LLC and WPP PLC

(b) County of Residence of First Listed Plaintiff Kings County
*(EXCEPT IN U.S. PLAINTIFF CASES)*

County of Residence of First Listed Defendant New York County
*(IN U.S. PLAINTIFF CASES ONLY)*
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Kim E. Richman, REESE RICHMAN LLP, 875 Avenue of the Americas
18th Floor, New York, New York 10001
Telephone: (212) 643-0500, Facsimile: (212) 253-4272

Attorneys *(If Known)*

CV 12 - 2674

KUNTZ, J.

ORENSTEIN, M.J.

**II. BASIS OF JURISDICTION** *(Place an "X" in One Box Only)*

□ 1 U.S. Government Plaintiff
□ 2 U.S. Government Defendant
□ 3 Federal Question *(U.S. Government Not a Party)*
☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

**III. CITIZENSHIP OF PRINCIPAL PARTIES** *(Place an "X" in One Box for Plaintiff and One Box for Defendant)* *(For Diversity Cases Only)*

| | PTF | DEF | | PTF | DEF |
|---|---|---|---|---|---|
| Citizen of This State | □ 1 | □ 1 | Incorporated *or* Principal Place of Business In This State | □ 4 | ☒ 4 |
| Citizen of Another State | ☒ 2 | □ 2 | Incorporated *and* Principal Place of Business In Another State | □ 5 | □ 5 |
| Citizen or Subject of a Foreign Country | □ 3 | □ 3 | Foreign Nation | □ 6 | □ 6 |

**IV. NATURE OF SUIT** *(Place an "X" in One Box Only)*

**CONTRACT**
□ 110 Insurance
□ 120 Marine
□ 130 Miller Act
□ 140 Negotiable Instrument
□ 150 Recovery of Overpayment & Enforcement of Judgment
□ 151 Medicare Act
□ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
□ 153 Recovery of Overpayment of Veteran's Benefits
□ 160 Stockholders' Suits
□ 190 Other Contract
□ 195 Contract Product Liability
□ 196 Franchise

**REAL PROPERTY**
□ 210 Land Condemnation
□ 220 Foreclosure
□ 230 Rent Lease & Ejectment
□ 240 Torts to Land
□ 245 Tort Product Liability
□ 290 All Other Real Property

**TORTS**

PERSONAL INJURY
□ 310 Airplane
□ 315 Airplane Product Liability
□ 320 Assault, Libel & Slander
□ 330 Federal Employers' Liability
□ 340 Marine
□ 345 Marine Product Liability
□ 350 Motor Vehicle
□ 355 Motor Vehicle Product Liability
□ 360 Other Personal Injury
□ 362 Personal Injury - Med. Malpractice

PERSONAL INJURY
□ 365 Personal Injury - Product Liability
□ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
□ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
□ 370 Other Fraud
□ 371 Truth in Lending
□ 380 Other Personal Property Damage
□ 385 Property Damage Product Liability

**CIVIL RIGHTS**
□ 440 Other Civil Rights
□ 441 Voting
□ 442 Employment
□ 443 Housing/ Accommodations
□ 445 Amer. w/Disabilities - Employment
□ 446 Amer. w/Disabilities - Other
□ 448 Education

**PRISONER PETITIONS**
□ 510 Motions to Vacate Sentence
**Habeas Corpus:**
□ 530 General
□ 535 Death Penalty
□ 540 Mandamus & Other
□ 550 Civil Rights
□ 555 Prison Condition
□ 560 Civil Detainee - Conditions of Confinement

**FORFEITURE/PENALTY**
□ 625 Drug Related Seizure of Property 21 USC 881
□ 690 Other

**LABOR**
□ 710 Fair Labor Standards Act
□ 720 Labor/Mgmt. Relations
□ 740 Railway Labor Act
□ 751 Family and Medical Leave Act
□ 790 Other Labor Litigation
□ 791 Empl. Ret. Inc. Security Act

**IMMIGRATION**
□ 462 Naturalization Application
□ 463 Habeas Corpus - Alien Detainee (Prisoner Petition)
□ 465 Other Immigration Actions

**BANKRUPTCY**
□ 422 Appeal 28 USC 158
□ 423 Withdrawal 28 USC 157

**PROPERTY RIGHTS**
□ 820 Copyrights
□ 830 Patent
□ 840 Trademark

**SOCIAL SECURITY**
□ 861 HIA (1395ff)
□ 862 Black Lung (923)
□ 863 DIWC/DIWW (405(g))
□ 864 SSID Title XVI
□ 865 RSI (405(g))

**FEDERAL TAX SUITS**
□ 870 Taxes (U.S. Plaintiff or Defendant)
□ 871 IRS—Third Party 26 USC 7609

**OTHER STATUTES**
□ 375 False Claims Act
□ 400 State Reapportionment
□ 410 Antitrust
□ 430 Banks and Banking
□ 450 Commerce
□ 460 Deportation
□ 470 Racketeer Influenced and Corrupt Organizations
□ 480 Consumer Credit
□ 490 Cable/Sat TV
□ 850 Securities/Commodities/ Exchange
☒ 890 Other Statutory Actions
□ 891 Agricultural Acts
□ 893 Environmental Matters
□ 895 Freedom of Information Act
□ 896 Arbitration
□ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
□ 950 Constitutionality of State Statutes

**V. ORIGIN** *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding
□ 2 Removed from State Court
□ 3 Remanded from Appellate Court
□ 4 Reinstated or Reopened
□ 5 Transferred from another district *(specify)*
□ 6 Multidistrict Litigation

**VI. CAUSE OF ACTION**
Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. § 1332(d)
Brief description of cause:
Unauthorized access to technological devices

**VII. REQUESTED IN COMPLAINT:**
☑ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23
DEMAND $
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes □ No

**VIII. RELATED CASE(S) IF ANY** *(See instructions)*:
JUDGE
DOCKET NUMBER

DATE
05/25/2012

SIGNATURE OF ATTORNEY OF RECORD
K. E. R.

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

EDNY

## CERTIFICATION OF ARBITRATION ELIGIBILITY

Local Arbitration Rule 83.10 provides that with certain exceptions, actions seeking money damages only in an amount not in excess of $150,000, exclusive of interest and costs, are eligible for compulsory arbitration. The amount of damages is presumed to be below the threshold amount unless a certification to the contrary is filed.

I, Kim E. Richman, counsel for Plaintiffs, do hereby certify that the above captioned civil action is ineligible for compulsory arbitration for the following reason(s):

☒ monetary damages sought are in excess of $150,000, exclusive of interest and costs,

☒ the complaint seeks injunctive relief,

□ the matter is otherwise ineligible for the following reason

## DISCLOSURE STATEMENT - FEDERAL RULES CIVIL PROCEDURE 7.1

Identify any parent corporation and any publicly held corporation that owns 10% or more or its stocks:

## RELATED CASE STATEMENT (Section VIII on the Front of this Form)

Please list all cases that are arguably related pursuant to Division of Business Rule 50.3.1 in Section VIII on the front of this form. Rule 50.3.1 (a) provides that "A civil case is "related" to another civil case for purposes of this guideline when, because of the similarity of facts and legal issues or because the cases arise from the same transactions or events, a substantial saving of judicial resources is likely to result from assigning both cases to the same judge and magistrate judge." Rule 50.3.1 (b) provides that " A civil case shall not be deemed "related" to another civil case merely because the civil case: (A) involves identical legal issues, or (B) involves the same parties." Rule 50.3.1 (c) further provides that "Presumptively, and subject to the power of a judge to determine otherwise pursuant to paragraph (d), civil cases shall not be deemed to be "related" unless both cases are still pending before the court."

## NY-E DIVISION OF BUSINESS RULE 50.1(d)(2)

1.) Is the civil action being filed in the Eastern District removed from a New York State Court located in Nassau or Suffolk County: No

2.) If you answered "no" above:
a) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in Nassau or Suffolk County? No

b) Did the events of omissions giving rise to the claim or claims, or a substantial part thereof, occur in the Eastern District? Yes

If your answer to question 2 (b) is "No," does the defendant (or a majority of the defendants, if there is more than one) reside in Nassau or Suffolk County, or, in an interpleader action, does the claimant (or a majority of the claimants, if there is more than one) reside in Nassau or Suffolk County?____________________
(Note: A corporation shall be considered a resident of the County in which it has the most significant contacts).

## BAR ADMISSION

I am currently admitted in the Eastern District of New York and currently a member in good standing of the bar of this court.
☒ Yes □ No

Are you currently the subject of any disciplinary action (s) in this or any other state or federal court?
□ Yes (If yes, please explain) ☒ No

I certify the accuracy of all information provided above.

Signature:______________________________

# EXHIBIT B

CV 12-2672

SUMMONS ISSUED

GARAUFIS, J.

ORENSTEIN, M.J.

**REESE RICHMAN LLP**
Kim E. Richman
krichman@reeserichman.com
Michael R. Reese
mreese@reeserichman.com
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643-0500
Facsimile: (212) 253-4272

- and -

**MILBERG LLP**
Sanford P. Dumain
sdumain@milberg.com
Peter E. Seidman
pseidman@milberg.com
One Penn Plaza
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

*Attorneys for Plaintiffs and the Proposed Class*

**UNITED STATES DISTRICT COURT**

**EASTERN DISTRICT OF NEW YORK**

| | |
|---|---|
| DANIEL MAZZONE and MICHELLE KUSWANTO, on behalf of themselves and all others similarly situated,<br>Plaintiffs,<br>vs.<br>VIBRANT MEDIA INC.,<br>Defendant. | Case No. ____________<br>**CLASS ACTION COMPLAINT**<br>**DEMAND FOR JURY TRIAL** |

Daniel Mazzone and Michelle Kuswanto (collectively, "Plaintiffs") allege the following, based upon personal knowledge and upon information and belief derived from, among other things, investigation of counsel and review of public documents.

## NATURE OF THE ACTION

1. This is a class action against Vibrant Media Inc. ("Vibrant" or "Defendant") arising from Defendant's hacking of computers and mobile devices and Defendant's invasion of Internet users' online privacy.

2. Defendant circumvented the privacy protections on Plaintiffs' Safari[1] web browsers, thereby hacking into Plaintiffs' computers and mobile devices (collectively, "Devices"). Subsequently, Defendant placed cookies on Plaintiffs' Safari browsers that Defendant used to obtain information about Plaintiffs and their Devices as they used Safari to browse web pages to which Defendant delivered web content as a third party. Included in the private information that Defendant obtained in this manner was sensitive, personal, and personally identifiable information, and, as set forth herein, Defendant, without Plaintiffs' knowledge, misappropriated and exploited this private information for its own uses.

3. These actions of Defendant violated New York General Business Law § 349; California Penal Code § 502; Article I, Section 1, of the California Constitution; and California Penal Code § 630 *et seq*. Defendant's conduct also constitutes trespass to personal property / chattels under New York common law and invasion of privacy under California common law.

## JURISDICTION AND VENUE

4. This Court has original jurisdiction over this class action under 28 U.S.C. § 1332(d), which, under the provisions of the Class Action Fairness Act ("CAFA"), explicitly provides for the original jurisdiction of the Federal Courts in any class action in which at least 100 members are in the proposed plaintiff class, any member of the plaintiff class is a citizen of a State different from any defendant, and the matter in controversy exceeds the sum of $5,000,000,

[1] All references to "Safari" are to the Safari web browser developed by Apple Inc.

exclusive of interest and costs. Plaintiffs allege that the total claims of individual members of the proposed Class are well in excess of $5,000,000 in the aggregate, exclusive of interest and costs.

5. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391. Substantial acts in furtherance of the alleged improper conduct, including hacking of Plaintiffs' and the Class members' Devices, occurred within this District.

## THE PARTIES

6. Plaintiff Daniel Mazzone resides in New York and uses his Devices there. Mr. Mazzone values his online privacy, especially when using the Internet in the seclusion of his home and/or when conducting his personal affairs. Mr. Mazzone browses the Internet using the Safari browser on both his iPad and computer. At all relevant times, Safari's "Third-Party-Blocking Only Option" (described in detail below) was either operating by default or had been selected by Mr. Mazzone. Mr. Mazzone used Safari to visit web pages that included advertisements (the "Hacking Ads", described in detail below) that Defendant used to hack into his Devices and, subsequently, to place tracking mechanisms called "cookies" on the Devices. Defendant used the cookies so placed, each of which was called "VM_USR", to obtain "End User Information" (as defined below) about Mr. Mazzone and his Devices as he used Safari to browse web pages to which Defendant delivered web content. In this manner, Defendant obtained private information about Mr. Mazzone and his Devices without his permission and against his will (as expressed by means of Safari's Third-Party-Blocking Only Option). Mr. Mazzone mistakenly believed that Safari's privacy controls protected him from having his information obtained by Defendant (in the manner described herein), and Mr. Mazzone mistakenly believed that Defendant's Hacking Ads were a benign part of the online environment. When Mr. Mazzone discovered that Defendant had hacked his Devices and learned and collected private information about him without his permission, Mr. Mazzone was shocked, humiliated, and angered and he suffered emotional distress. Furthermore, Defendant's conduct undermined Mr. Mazzone's faith and confidence in the trustworthiness and integrity of the Internet.

Defendant degraded the value of Mr. Mazzone's Devices and deprived him of the ability to sell to Defendant the information that Defendant collected against his will.

7. Plaintiff Michelle Kuswanto resides in California and uses her Devices there. Ms. Kuswanto values her online privacy, especially when using the Internet in the seclusion of her home and/or when conducting her personal affairs. Ms. Kuswanto browses the Internet using the Safari browser on both her iPhone and computer. At all relevant times, Safari's Third-Party-Blocking Only Option was either operating by default or had been selected by Ms. Kuswanto. Ms. Kuswanto used Safari to visit web pages that included Hacking Ads that Defendant used to hack into her Devices and, subsequently, to place the "VM_USR" cookie on the Devices. Defendant used the cookies so placed to obtain End User Information about Ms. Kuswanto and her Devices as she used Safari to browse web pages to which Defendant delivered web content. In this manner, Defendant obtained private information about Ms. Kuswanto and her Devices without her permission and against her will (as expressed by means of Safari's Third-Party-Blocking Only Option). Ms. Kuswanto mistakenly believed that Safari's privacy controls protected her from having her information obtained by Defendant (in the manner described herein), and Ms. Kuswanto mistakenly believed that Defendant's Hacking Ads were a benign part of the online environment. When Ms. Kuswanto discovered that Defendant had hacked her Devices and learned and collected private information about her without her permission, Ms. Kuswanto was shocked, humiliated, and angered and she suffered emotional distress. Furthermore, Defendant's conduct undermined Ms. Kuswanto's faith and confidence in the trustworthiness and integrity of the Internet. Defendant degraded the value of Ms. Kuswanto's Devices and deprived her of the ability to sell to Defendant the information that Defendant collected against her will. (Exhibit 1 hereto shows the results of a diagnostic test performed on Ms. Kuswanto's iPhone through the website of the Network Advertising Initiative, a self-regulatory organization comprised of over 80 online advertising companies, including Vibrant.)

8. Defendant Vibrant Media Inc. is a Delaware corporation that maintains its headquarters in New York, New York. Vibrant conducts business throughout New York, the nation, and internationally.

## STATEMENT OF THE CASE

9. People have incorporated the web into their personal lives, through the use of things like social media, dating sites, digital commerce, political forums, and sites containing medical information. *See* The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012) (Foreword), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

10. Plaintiffs at all relevant times used the Internet to communicate with others via social media, to engage in commerce, and to search for a wide variety of information, much of it personal, sensitive, and private. They often browsed the Internet from the seclusion of their homes and at all relevant times did not expect, nor did they have any reason to expect, that outsiders would observe or record their online activities.

11. This expectation derived, in part, from various mechanisms that are designed to grant Plaintiffs control over who may access information about them and their Devices as they browse the Internet.[2] These mechanisms include the privacy controls incorporated into Apple Inc.'s Safari web browser (the "Privacy Controls").[3] Safari's Privacy Controls are adjustable at the discretion of the Safari user. At all relevant times, Plaintiffs had available a choice:

(a) They could keep their "End User Information" (as defined below) secret from all websites.

[2] The "Do Not Track" system, which allows consumers to signal to online companies that they do not want to be tracked, is one such mechanism. *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* i, iii, v (Mar. 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[3] The Privacy Controls only protect Internet users when they are browsing using Safari. The Privacy Controls have no effect on and cannot protect browsing conducted using other web browsers, such as Windows Internet Explorer (developed by Microsoft Corporation) or Mozilla Firefox (developed by Mozilla Foundation and Mozilla Corporation).

(b) They could keep their End User Information secret from all websites except for the websites whose web pages they visited (the "First Party Content Providers"). For example, if a Safari user chose this option and then visited a web page on the site located at http://www.amazon.com/ ("amazon.com"), Safari would allow amazon.com to set cookies on the Safari user's Device.[4] If amazon.com then set a cookie(s) on the user's Device, amazon.com could use the cookie(s), among other things, to facilitate collection of End User Information about the Safari user whenever the user visited web pages that included content provided by amazon.com, [5] to streamline the purchase process, or to facilitate recommendation of products based on the user's amazon.com browsing and purchase history. Many Internet users are willing to allow First Party Content Providers to set cookies (and thereby potentially to obtain End User Information about them) because many web pages cannot function properly (or in some cases, at all) if the First Party Content Provider cannot set cookies. This option is the default option in Safari's Privacy Controls – *i.e.*, it is the one that is operational by default and remains in operation unless the Safari user switches to another option. Herein, this option is referred to as the "Third-Party-Blocking Only Option."

(c) They could allow not only First Party Content Providers but also "Third Party Content Providers" to set cookies on their Devices and thereby potentially obtain End User Information about them as they browse the web using Safari. A "Third Party Content Provider" is a website that

[4] In this instance, amazon.com is the website acting as the First Party Content Provider.

[5] Practically speaking, a website cannot efficiently and reliably collect End User Information about an Internet user without setting a cookie on the Internet user's Device.

delivers content to a web page that is part of a separate, different website, as an Internet user is visiting the page.[6] For example, when an Internet user is visiting a web page on the site located at http://www.facebook.com/ ("facebook.com"), the web page may include content (for example, an ad) delivered from the site located at http://www.third-party-advertiser.com/ ("third-party-advertiser.com"). In this instance, facebook.com is acting as a First Party Content Provider and third-party-advertiser.com is acting as a Third Party Content Provider. Herein, the content delivered by a Third Party Content Provider to a First Party Content Provider's web page is called "Third Party Content."[7]

12. A Safari user who has selected the Third-Party-Blocking Only Option can stop the Privacy Controls from keeping End User Information secret from a specific Third Party Content Provider by submitting an online form to that Third Party Content Provider (the "Form Exception").

13. As used herein, the term "End User Information" means information that a website can obtain about an Internet user after the site has set a cookie on the user's Device. The information may be obtained when the user visits either (i) a web page that is part of the site or (ii) a web page to which the site is delivering Third Party Content. End User Information includes but is not limited to the Uniform Resource Locator ("URL") of the page that the user visited (i) on the site or (ii) to which the site delivered Third Party Content; the time at which the user visited the page; details about the operating system on which the user's browser was running (for example, "Mac OS X" on an iPad); and details about the user's web browser (including information about extensions added to the browser). If a site sets a cookie on an

[6] The latter website is thus acting as a First Party Content Provider.

[7] Examples of Third Party Content include advertisements and "web beacons" (further explained herein).

Internet user's Device and the user subsequently visits a series of web pages that (i) are part of the site or (ii) are pages to which the site delivers Third Party Content, then the site can collect a list or a history of information about the user (including the information listed in this paragraph).

14. A website can thus collect End User Information about an Internet user when it provides Third Party Content to other sites throughout the web that the user visits, so long as the website has set a cookie on the user's Device. As noted in footnote 7, *supra*, Third Party Content includes but is not limited to ads and "web beacons." "Web beacons" are pieces of web content that are invisible (or extremely small).[8] When a website delivers a web beacon to a web page as Third Party Content, the Internet user visiting the page is almost always unaware that the web beacon is included on the page (unlike the case where an ad is delivered to a web page as Third Party Content). The purpose, however, of delivering a web beacon as Third Party Content to a web page is not for the Internet user visiting the page to see the web beacon. It is instead to allow the site delivering the web beacon to obtain End User Information about the user (which is, practically speaking, only possible when the Third Party Content Provider has set a cookie on the user's Device).

15. Few Internet users are willing to allow websites they have never directly visited to obtain End User Information about them, even if those sites have delivered Third Party Content to (first party) web pages that the users have visited.

16. Defendant's business includes delivering ads as Third Party Content to web pages throughout the World Wide Web on behalf of Defendant's advertiser clients.

17. Defendant's business also includes obtaining End User Information about Internet users as the users browse sites to which Defendant delivers Third Party Content (including ads

[8] Web beacons are alternatively known as "web bugs", "tags", "tracking pixels", "1 x 1 gifs", and "clear gifs". Vibrant's privacy statement explains that it uses web beacons in conjunction with cookies. *See* http://www.vibrantmedia.com/privacy.asp ("You may encounter our technology: … when one of our Clients places one of our web beacons on its website, which you visit. ***** Our Technology uses cookies in conjunction with Web beacons in order to help make the online advertisements you see more relevant to you.")

and web beacons), which is possible when Defendant has set cookies on the Internet users' Devices.

18. Defendant used computer programming language contained in some of the ads it delivered to web pages as Third Party Content (the "Hacking Ads") to disable the protection provided by Safari's Privacy Controls – the Safari users' express preference with regard to setting of cookies on their Devices, including cookies used to obtain End User Information – with respect to Defendant. *See infra* ¶ 11.

19. Specifically, when Defendant delivered a Hacking Ad as Third Party Content to a web page that was loading in a Plaintiff's or Class member's Safari browser, the computer programming language within the Hacking Ad caused the browser to *immediately* send an *invisible* online form back to Defendant, triggering Safari's Form Exception with respect to Defendant (*i.e.*, turning off Safari's privacy protections with respect to Defendant).

20. However, a Safari user is the only appropriate person to fill out and send this type of online form from the user's Device to Defendant, especially when doing so has the effect of disabling Safari's privacy protections with respect to Defendant. Defendant thus hacked Plaintiffs' and the Class members' Devices by means of the Hacking Ads.

21. After Defendant had hacked Plaintiffs' and the Class members' Devices, Safari's Privacy Controls no longer prevented Defendant from setting cookies on Plaintiffs and the Class members Devices, including cookies that Defendant could use in conjunction with Third Party Content (as described above) to obtain End User Information about Plaintiffs and the Class members.

22. Specifically, once Defendant had triggered Safari's Form Exception, Defendant was able to and did place the "VM_USR" cookie on the Device that was hacked. Each "VM_USR" cookie contains an ID that Vibrant uses for tracking purposes.

23. Stanford researcher Jonathan Mayer first identified Defendant's Hacking Ads. Mr. Mayer's blog describes these findings in detail. *See* http://webpolicy.org/2012/02/17/safari-trackers/. Subsequently, Ashkan Soltani, technology adviser for *The Wall Street Journal*,

independently confirmed Mr. Mayer's findings. Mr. Soltani surveyed the top 100 most popular websites as ranked by Quantcast in February 2012.

24. On February 17, 2012, *The Wall Street Journal* published an article describing Mr. Mayer's and Mr. Soltani's findings in detail. *See* Julia Angwin & Jennifer Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, Wall St. J., Feb. 17, 2012, *available at* http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

25. According to *The Wall Street Journal*, Vibrant has admitted to using Hacking Ads to enable placement of ID cookies that enable it to obtain End User Information about Safari users. *The Wall Street Journal* states:

> A Vibrant Media spokesman called its use of the [Privacy Controls circumvention] technique a "workaround" to "make Safari work like all the other browsers." Other major Web browsers don't block tracking by default. Vibrant, a top 25 ad network in the U.S. according to comScore Media Metrix, uses the technique "for unique user identification," the spokesman said, but doesn't collect personally identifiable information such as name or financial-account numbers.

Angwin & Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy.*

26. Mr. Mayer discovered Defendant's Hacking Ads on the following sites:
http://answers.com/
http://cbslocal.com/ [various region-specific subdomains]

27. At all relevant times, Plaintiffs were unaware that Defendant had improperly disabled their Safari privacy protections to allow Defendant to collect and exploit End User Information about them, including their private Internet browsing history.

28. To prevent this, Plaintiffs and the Class members could have deleted the "VM_USR" cookie or visited certain websites and opted out of tracking by Defendant. Plaintiffs and the Class members, however, did not know that the "VM_USR" cookie was on their Devices or that Defendant was obtaining End User Information about them as they surfed the web. Plaintiffs and the Class members instead believed that Safari's Privacy Controls, which were set to the Third-Party-Blocking Only Option, prevented Third Party Content Providers (including

Defendant when it was acting as a Third Party Content Provider) from placing cookies on their Devices and obtaining End User Information about them. Plaintiffs and the Class members therefore had no reason to locate and delete the "VM_USR" cookie or to attempt to discover which websites they could use to opt out of tracking by Defendant.

29. Defendant injured Plaintiffs and the Class members by hacking their Devices.

30. As a result of being hacked, the Devices no longer functioned as they normally should have.

31. By hacking the Devices and impairing their functionality, Defendant degraded their value.

32. Upon discovering that Defendant had hacked their Devices and obtained private End User Information about them without their permission and against their will (as expressed by means of Safari's Third-Party-Blocking Only Option), Plaintiffs and the Class members were shocked, humiliated, and angered, and suffered emotional distress.

33. By the above actions, Defendant undermined Plaintiffs' and the Class members' confidence in the safety and trustworthiness of the digital environment.

**The Value of People's Personal Information**

34. The personal information that Defendant collected is an asset that is priced, bought, and sold in discrete units for marketing and other purposes. "Websites and stores can . . . easily buy and sell information on valued visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them." Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, & Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214. The more information that is known about a consumer, the more a company will pay to deliver a precisely targeted advertisement to him or her. *See* Federal Trade Commission (FTC), Protecting Consumer Privacy in an Era of Rapid Change, Preliminary Staff Report (Dec. 2010) ("FTC Report"), at 24.

35. Personal data is viewed as currency. "In many instances, consumers pay for free content and services by disclosing their personal information," according to former FTC commissioner Pamela Jones Harbour. FTC Roundtable Series 1 on: Exploring Privacy (Matter No. P095416) (Dec. 7, 2009), at 148, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/ PrivacyRoundtable_Dec 2009_Transcript.pdf. In *Property, Privacy, and Personal Data*, Professor Paul M. Schwartz wrote:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

36. On February 28, 2011, *The Wall Street Journal* highlighted a company called "Allow Ltd.," which is one of nearly a dozen companies that offers to sell people's personal information on their behalf and which gives its users 70% of such sales. *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, Wall St. J., Feb. 28, 2011, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html. For example, one Allow Ltd. user received a payment of $8.95 for letting Allow tell a credit card company the user was shopping for a new credit card. *Id.*

37. On February 15, 2012, *The Financial Times* acknowledged the value of personal information in the Internet age in the context of Facebook, Inc.'s upcoming initial public offering: "Two weeks ago Facebook announced an initial public offering that could value the company at up to $100bn. Facebook is worth so much because of the data it holds on its 845m users."[9]

[9] Richard Falkenrath, *Google Must Remember Our Right to be Forgotten*, Fin. Times, *available at* http://www.ft.com/intl/cms/s/0/476b9a08-572a-11e1-869b-00144feabdc0.html#axzz1mgPiI5Ux.

38. As noted in *The Wall Street Journal*, "[t]rade in personal data has emerged as a driver of the digital economy. Many tech companies offer products for free and get income from online ads that are customized using data about customers. These companies compete for ads, in part, based on the quality of the information they possess about users." Angwin & Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*.

39. Google Inc. ("Google") also acknowledges the value of web browsing histories by purchasing such histories directly from web users. Google's "Screenwise" panel is a program whereby a few thousand Google users are allowing Google to track their web browsing histories in return for up to $25 in gift cards. *See* http://www.google.com/landing/screenwisepanel/.

40. Defendant ultimately profited from using the information they collected after hacking Plaintiffs' and the Class members' Devices in, among other things, its online advertising business.

41. By the above actions, Defendant deprived Plaintiffs and the Class members of the ability to sell their personal information, including web browsing histories, to Defendant.

## **CLASS ACTION ALLEGATIONS**

42. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a class of Internet users (collectively, the "Class") defined as follows:

> All Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that disabled their Privacy Controls with respect to Defendant, enabling Defendant to place the "VM_USR" cookie on the users' Devices, and (3) on whose Devices Defendant then placed the "VM_USR" cookie. The class period runs from the date that Defendant first began delivering Hacking Ads to web pages to the date of filing of this complaint (the "Class Period").

43. Plaintiffs also bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a subclass of Internet users residing in New York (collectively, the "New York Subclass") defined as follows:

> All New York Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that disabled their Privacy Controls with respect to Defendant, enabling Defendant to place the "VM_USR" cookie on the users' Devices, and (3) on whose Devices Defendant then placed the "VM_USR" cookie; during the Class Period.

44. Plaintiffs also bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a subclass of Internet users residing in California (collectively, the "California Subclass") defined as follows:

> All California Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that hacked their Privacy Controls, enabling Defendant to place the "VM_USR" cookie on the users' Devices, and (3) on whose Devices Defendant then placed the "VM_USR" cookie; during the Class Period.

45. Excluded from the Class are Defendant; any parent, subsidiary, or affiliate of Defendant or any employees, officers, or directors of Defendant; legal representatives, successors, or assigns of Defendant; and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

46. **Numerosity**. The Class members are so numerous and dispersed nationwide that joinder of all members is impracticable. Upon information and belief, there are millions of Internet users whose Safari Privacy Controls have been debilitated by Defendant's Hacking Ads. The exact number of Class members is unknown, but Plaintiffs reasonably estimate and believe that there are millions of persons in the Class.

47. **Commonality**. There are numerous and substantial questions of law and fact that are common to all members of the Class, which predominate over any question affecting only individual Class members. The members of the Class were and potentially continue to be subjected to the same practices of Defendant. The common questions and issues raised by Plaintiffs' claims include, *inter alia*, the following:

(a) whether Defendant hacked Plaintiffs' and the Class members' Devices using Hacking Ads; and

(b) whether Defendant collected Plaintiffs and the Class members' web browsing histories against their will.

48. **Typicality**. Plaintiffs' claims are typical of the claims of all of the other members of the Class, because their claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendant.

49. **Adequacy**. Plaintiffs will fairly and adequately protect the interests of all members of the Class in the prosecution of this action and in the administration of all matters relating to the claims stated herein. Plaintiffs are similarly situated with, and have suffered similar injuries to, the members of the Class they seek to represent. Plaintiffs have retained counsel experienced in handling class action lawsuits. Neither Plaintiffs nor their counsel have any interest that might cause them not to vigorously pursue this action.

50. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy, since individual joinder of the Class members is impracticable. Even if individual Class members were able to afford individual litigation, it would be unduly burdensome to the Courts in which the individual litigation would proceed. Defendant has subjected the Class to the same violations as referenced herein. Accordingly, class certification is appropriate under Rule 23 because common issues of law and fact regarding Defendant's uniform violations predominate over individual issues, and class certification is a superior method of resolving these claims. No unusual difficulties are likely to be encountered in the management of this action as a class action. Defendant has acted in a manner that affects Plaintiffs and all Class members alike, thereby making appropriate injunctive, declaratory, and other relief appropriate with respect to the Class as a whole.

## CAUSES OFACTION

### COUNT ONE

### (VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349)

51. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

52. New York General Business Law § 349 prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state…."

53. In violation of § 349, Defendant engaged in material, deceptive, consumer-oriented acts in the conduct of business that injured Plaintiffs and the Class members.

54. Specifically, Plaintiffs and the Class members mistakenly believed that viewing web pages that included Hacking Ads would not harm their Devices.

55. Defendant's Hacking Ads appeared to be a non-invasive, benign part of the digital environment.

56. In reality, Defendant used its Hacking Ads to harm Plaintiffs' and the Class members' Devices by debilitating the functionality of their Safari Privacy Controls, as described herein.

57. Further, Plaintiffs and the Class members mistakenly believed that Defendant would respect that they, via Safari's Privacy Controls, had explicitly denied permission to Defendant to use Third Party Content in conjunction with cookies to obtain End User Information about them.

58. In reality, Defendant ignored Plaintiffs' and the Class members' explicit prohibition, disabled the functionality of Safari's Privacy Controls, and used its Third Party Content in conjunction with cookies it set on Plaintiffs' and the Class members' Devices to obtain End User Information about Plaintiffs and the Class members as they visited web pages throughout the web.

59. Defendant's acts and/or omissions were generally aimed at the consuming public.

60. These unlawful deceptive acts directly and proximately caused harm to Plaintiffs and the Class members in the following ways:

(a) through the degradation in value of their Devices;

(b) through the loss of their privacy and the exposure of their personal, sensitive, and private information, as a result of which Plaintiffs and the Class members were shocked, humiliated, and angered and suffered emotional distress;

(c) by depriving Plaintiffs and the Class members of the ability to sell their personal information, including their web browsing histories, to Defendant.

61. As a direct and proximate result of Defendant's violation of § 349, Plaintiffs and the Class members have suffered damages in an amount to be determined at trial.

62. Plaintiffs and the Class members have also suffered irreparable injury as a result of Defendant's unlawful conduct, including the unauthorized collection of their personal information. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class members have no adequate remedy at law, entitling them to injunctive relief.

## COUNT TWO

## (VIOLATION OF THE CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CALIFORNIA PENAL CODE § 502)

63. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

64. California Penal Code § 502(c)(1) prohibits a person from knowingly accessing and without permission altering, damaging, and/or otherwise using data, computers, computer systems, and/or computer networks to:

(A) execute a scheme or artifice to defraud or deceive, and/or

(B) wrongfully control or obtain money, property, or data.

65. In violation of § 502(c)(1), Defendant intentionally and without permission altered, damaged, and otherwise used Plaintiffs' and the Class members' Devices to execute a scheme or artifice to defraud or deceive.

66. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Devices as part of the execution of a scheme in which Defendant intentionally failed to inform Plaintiffs and the Class members that Defendant had hacked their Devices and

subsequently used Third Party Content in conjunction with cookies to End User Information about Plaintiffs and the Class members as they surfed the web.

67. In violation of § 502(c)(1), Defendant intentionally and without permission altered, damaged, and otherwise used Plaintiffs' and the Class members' Devices to wrongfully control or obtain money, property, or data.

68. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Devices without their knowledge to obtain personal data about them, including their web browsing histories. Further, the personal data that Defendant obtained is property.

69. California Penal Code § 502(c)(2) prohibits a person from knowingly accessing and without permission taking, copying, and/or making use of data from a computer, computer system, and/or computer network.

70. In violation of § 502(c)(2), Defendant intentionally and without permission took, copied, and/or made use of data from Plaintiffs' and the Class members' Devices.

71. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Devices and took information about their web surfing from the Devices, which Defendant made use of in its advertising business.

72. California Penal Code § 502(c)(3) prohibits a person from knowingly and without permission using "computer services" as that term is defined in California Penal Code § 502(b)(4).

73. In violation of § 502(c)(3), Defendant intentionally and without permission used "computer services," including but not limited to storage functions and web history tracking.

74. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Devices, stored cookies on the Devices, and used those cookies in conjunction with browser software on the Devices to obtain End User Information about Plaintiffs and the Class members as they browsed web pages to which Defendant delivered Third Party Content.

75. California Penal Code § 502(c)(4) prohibits a person from knowingly and without permission adding, altering, and/or damaging data, computer software, and/or computer

programs that reside and/or exist internal and/or external to a computer, computer system, and/or computer network.

76. In violation of § 502(c)(4), Defendant intentionally and without permission added, altered, and/or damaged data, computer software, and/or computer programs that resided internal to Plaintiffs' and the Class members' Devices.

77. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Safari Privacy Controls, debilitating their functionality.

78. Further, Defendant intentionally and without permission added cookies to Plaintiffs' and the Class members' Devices.

79. California Penal Code § 502(c)(5) prohibits a person from knowingly and without permission disrupting and/or causing the disruption of "computer services" (as that term is defined in California Penal Code § 502(b)(4)) to an authorized user of a computer, computer system, and/or computer network.

80. In violation of § 502(c)(5), as described in detail herein, Defendant disabled the functionality of Plaintiffs' and the Class members' Safari Privacy Controls, thereby disrupting Plaintiffs' and the Class members' desired use of their web browsers and the World Wide Web.

81. California Penal Code § 502(c)(7) prohibits a person from knowingly and without permission accessing computers, computer systems, and/or computer networks.

82. In violation of § 502(c)(7), as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Safari Privacy Controls and placed cookies on their Devices, which Defendant used in conjunction with Third Party Content to obtain End User Information about them as they surfed the web.

83. California Penal Code § 502(c)(8) prohibits a person from knowingly introducing "computer contaminants" – as defined in California Penal Code § 502(b)(10) – into computers, computer systems, and/or computer networks.

84. In violation of § 502(c)(8), as described in detail herein, Defendant intentionally introduced computer programming code into Plaintiffs' and the Class members' Devices that

"usurp[ed] the normal operation" of the Devices by hacking Safari's Privacy Controls, enabling the placement of cookies on the Devices.

85. As a direct and proximate result of Defendant's violation of California Penal Code § 502, Defendant caused loss to Plaintiffs and the Class members in an amount to be proven at trial.

86. Plaintiffs and the Class members are entitled to recovery of attorneys' fees pursuant to § 502(e).

87. Plaintiffs and the Class members are entitled to punitive or exemplary damages under California Penal Code § 502(e)(4) because Defendant willfully violated § 502(c) and is guilty of "fraud" as defined by California Civil Code § 3294(c)(3).

88. Under § 3294(c)(3), "fraud" means an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury.

89. As described in detail herein, Defendant intentionally concealed from Plaintiffs and the Class members the fact that Defendant dismantled the privacy safeguards established by their Privacy Controls.

90. As a result of concealing this fact, Defendant intended to and did deprive Plaintiffs and the Class members of their legal right to privacy.

91. Further, as a result of concealing this fact, Defendant intended to profit and did profit by obtaining without authorization personal, private, and sensitive information about Plaintiffs and the Class members as they surfed the web and using the information in connection with Defendant's advertising business. Defendant's actions deprived Plaintiffs and the Class of the opportunity to sell the information to Defendant. Defendant thereby deprived Plaintiffs and the Class members of valuable property.

92. Plaintiffs and the Class members have also suffered irreparable injury as a result of Defendant's unlawful conduct, including the unauthorized collection of their personal information. Additionally, because the stolen information cannot be returned, the harm from the

security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class members have no adequate remedy at law, entitling them to injunctive relief.

## COUNT THREE

## (VIOLATION OF ARTICLE I, SECTION 1 OF THE CALIFORNIA CONSTITUTION)

93. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

94. Article I, Section 1 of the California Constitution states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

95. Plaintiffs and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their Devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy controls.

96. Plaintiffs and the Class members have a legally protected privacy interest in the End User Information (including personal, confidential, and sensitive information and web browsing histories) that Defendant obtained by hacking Plaintiffs' and the Class members' Safari Privacy Controls.

97. Plaintiffs and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their Devices free of interference, including decisions related to web browser privacy controls.

98. Plaintiffs and the Class members reasonably expected that their End User Information (including personal, confidential, and sensitive information) and intimate personal decisions would be kept private.

99. Defendant committed a serious invasion of Plaintiffs' and the Class members' privacy interests by hacking their Safari Privacy Controls. Unbeknownst to Plaintiffs and Class

members, Defendant made a private decision on behalf of Plaintiffs and the Class members that Defendant was not authorized to make.

100. Defendant committed a serious invasion of Plaintiffs' and the Class members' privacy interests by, after hacking their Safari Privacy Controls, obtaining End User Information (including personal, confidential, and sensitive information) about them as they surfed the web without authorization.

101. By the acts, transactions, and courses of conduct alleged herein, Defendant violated Plaintiffs' and the Class members' inalienable right to privacy.

102. As a consequence, Plaintiffs and the Class members were personally injured and suffered emotional distress damages.

**COUNT FOUR**

**(VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT, CALIFORNIA PENAL CODE § 630 *ET SEQ.*)**

103. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

104. In violation of California Penal Code § 631, Defendant, by means of a contrivance (or in "any other manner") made an unauthorized connection, electrically or "otherwise", with the wires, lines, cables, or instruments within the State of California over which communications or messages traveled between Plaintiffs' and the Class members' web browsers and the websites whose web pages they visited.

105. Specifically, as described in detail herein, Defendant hacked Plaintiffs' and the Class members' Safari Privacy Controls, which enabled it to place cookies on Plaintiffs' and the Class members' devices that it was explicitly not authorized to place. The cookies so placed, when used in conjunction with delivery of Third Party Content to Plaintiffs and the Class members (as described above), enabled Defendant to obtain End User Information about Plaintiffs and the Class members that Defendant would not otherwise have been able to obtain. Accordingly, Defendant created an unauthorized connection to Plaintiffs' and the Class

members' communications with the websites whose web pages they visited, which occurred over wires, lines, cables, or instruments within the State of California.

106. In violation of California Penal Code § 631, Defendant willfully, intentionally, without the consent of Plaintiffs and the Class members, and in an unauthorized manner, obtained, read, attempted to read, learned, and/or attempted to learn the contents of Plaintiffs' and the Class members' electronic communications with (or messages to) the websites whose web pages they visited while the communications (or messages) were in transit in or through California and/or while they were being sent from or received at a place within California.

107. Further, websites whose web pages were visited by Plaintiffs and the Class members did not have the authority to consent to alteration by Defendant of Plaintiffs' and the Class members' Safari Privacy Controls.

108. Defendant used and communicated such illegally obtained electronic communications of Plaintiffs and the Class members, including use and communication in its online advertising business.

109. As a direct and proximate result of the above-described conduct by Defendant, Plaintiffs and all Class members have suffered, and, unless such conduct is enjoined, will continue to suffer, damages in an amount to be proven at trial.

110. Pursuant to California Penal Code § 637.2, Plaintiffs and the Class members are entitled to recover three times their actual and/or statutory damages from Defendant, for the conduct described herein.

111. Defendant's conduct is causing, and unless enjoined will continue to cause, Plaintiffs and the Class members great and irreparable injury that cannot be fully compensated for or measured in money. Plaintiffs and the Class members have no adequate remedy at law and, pursuant to California Penal Code § 637.2(b), are entitled to preliminary and permanent injunctions prohibiting further use and communication of their unlawfully obtained information.

## COUNT FIVE

## (TRESPASS TO PERSONAL PROPERTY / CHATTELS)

112. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

113. The common law of New York prohibits the intentional intermeddling with personal property in possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

114. In violation of New York common law and as detailed more fully herein, Defendant dispossessed Plaintiffs and the Class members from use and/or access to their Devices, or parts of them, without their knowledge or consent. Further, Defendant's acts constituted an intentional interference with the use and enjoyment of the Devices.

115. Without Plaintiffs' and the Class members' knowledge or consent, Defendant knowingly and intentionally accessed their property and caused them injury.

116. Defendant engaged in deception and concealment in order to gain access to Plaintiffs' and the Class members' Devices.

117. Defendant's hacking of Safari's Privacy Controls and subsequent installation of cookies on Plaintiffs' and the Class members' Devices interfered and/or intermeddled with the Devices, including by altering or damaging controls designed to prevent the information collection effected by Defendant. Such use, interference, and/or intermeddling was without the knowledge or consent of Plaintiffs and the Class members.

118. Defendant's hacking of Plaintiffs' and the Class members' Devices and subsequent placement of cookies on them impaired their condition and value. In particular, these actions debilitated the functionality of Plaintiffs' and the Class members' Safari Privacy Controls.

119. Defendant's trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and the Class members.

120. As a direct and proximate result of Defendant's trespass to chattels, nuisance, interference, and unauthorized access to and intermeddling with Plaintiffs' and the Class members' Devices, Defendant has injured and impaired the condition and value of the Devices as follows:

(a) By consuming the resources of and/or degrading the performance of Plaintiffs' and the Class members' Devices (including space, memory, processing cycles, and Internet connectivity);

(b) By diminishing the use of, value, speed, capacity, and/or capability of Plaintiffs' and the Class members' Devices;

(c) By altering and controlling the functioning of Plaintiffs' and the Class members' Devices;

(d) By devaluing, interfering with, and/or diminishing Plaintiffs' and the Class members' possessory interest in their Devices;

(e) By infringing on Plaintiffs' and the Class members' right to exclude others from their Devices;

(f) By infringing on Plaintiffs' and the Class members' right to determine, as owners of their Devices, which programs should be installed and operated on the Devices, and how programs should be installed and operated on the Devices;

(g) By compromising the integrity, security, and ownership of Plaintiffs' and the Class members' Devices;

(h) By forcing Plaintiffs and the Class members to expend time and resources in order to remove the cookies installed on their Devices without notice or consent.

121. Plaintiffs and the Class members have no adequate remedy at law.

## COUNT SIX

## (INVASION OF PRIVACY IN VIOLATION OF CALIFORNIA COMMON LAW)

122. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

123. Defendant intruded on Plaintiffs' and the Class members' private affairs and seclusion by hacking their Safari Privacy Controls and placing cookies on their Devices – conduct that Defendant engaged in completely outside of their knowledge and against their express will. The cookies enabled Defendant, without authorization, to obtain End User Information about Plaintiffs and the Class members as they surfed the web, as more fully detailed herein.

124. Plaintiffs and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their Devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy controls.

125. Plaintiffs and the Class members have a legally protected privacy interest in the End User Information (including personal, confidential, and sensitive information and web browsing histories) that Defendant obtained by hacking Plaintiffs' and the Class members' Safari Privacy Controls.

126. Plaintiffs and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their Devices free of interference, including decisions related to web browser privacy controls.

127. Plaintiffs and the Class members reasonably expected that their End User Information (including personal, confidential, and sensitive information) and intimate personal decisions would be kept private.

128. Defendant intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by hacking Plaintiffs' and the Class members' Safari Privacy Controls. Unbeknownst to Plaintiffs and the Class members, Defendant made a private

decision on behalf of Plaintiffs and the Class members that Defendant was not authorized to make.

129. Defendant intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by, after hacking Plaintiffs' and the Class members' Safari Privacy Controls, obtaining End User Information about them as they surfed the web without authorization.

130. As a consequence, Plaintiffs and the Class members were personally injured and suffered emotional distress damages.

## PRAYER FOR RELIEF

**WHEREFORE,** Plaintiffs and members of the Class seek relief against Defendant as follows:

A. An order certifying that this action is properly brought and may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs be appointed as Class Representatives, and that Plaintiffs' counsel be appointed Class Counsel.

B. Awarding damages as alleged above.

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class members, including, *inter alia*, an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein.

D. Disgorgement of all revenue earned from selling or otherwise using or trading on the private information obtained from Plaintiffs and the Class members as a result of hacking their Devices, as described herein.

E. Awarding Plaintiffs and the Class members their reasonable litigation expenses and attorneys' fees; and

F. Awarding such other and further relief at law or equity as this court may deem just and proper.

## DEMAND FOR JURY TRIAL

Plaintiffs and the Class members hereby demand trial of their claims by jury to the extent authorized by law.

DATED: May 25, 2012

**REESE RICHMAN LLP**

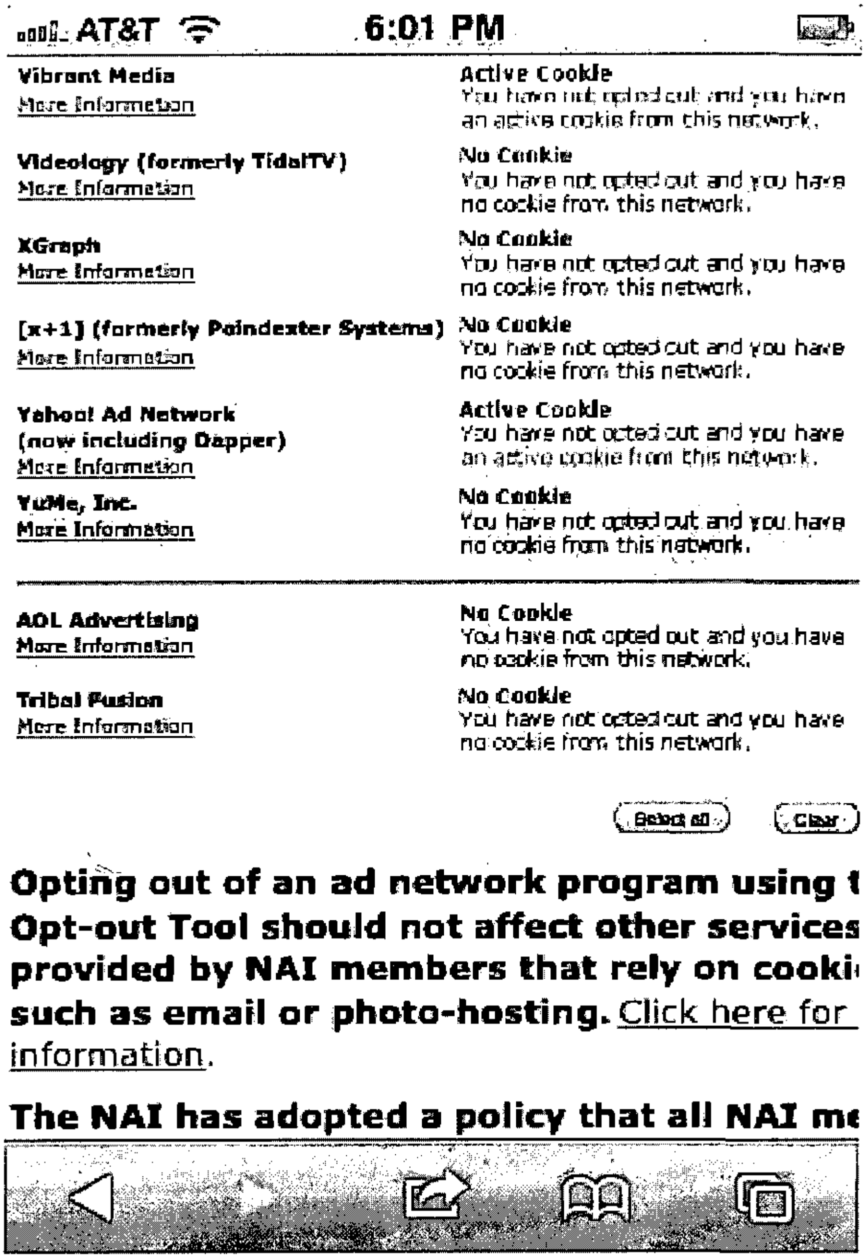
Kim E. Richman
krichman@reeserichman.com
Michael R. Reese
mreese@reeserichman.com
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643-0500
Facsimile: (212) 253-4272

– and –

**MILBERG LLP**
Sanford P. Dumain
sdumain@milberg.com
Peter Seidman
pseidman@milberg.com
One Penn Plaza
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

*Attorneys for Plaintiffs and the Proposed Class*

# EXHIBIT 1



| | |
|---|---|
| **Vibrant Media**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. |
| **Videology (formerly TidalTV)**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. |
| **XGraph**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. |
| **[x+1] (formerly Poindexter Systems)**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. |
| **Yahoo! Ad Network (now including Dapper)**<br>More Information | **Active Cookie**<br>You have not opted out and you have an active cookie from this network. |
| **YuMe, Inc.**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. |
| **AOL Advertising**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. |
| **Tribal Fusion**<br>More Information | **No Cookie**<br>You have not opted out and you have no cookie from this network. |

**Opting out of an ad network program using t Opt-out Tool should not affect other services provided by NAI members that rely on cooki such as email or photo-hosting.** Click here for information.

**The NAI has adopted a policy that all NAI me**

EXHIBIT C

**BEFORE THE UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION**

| | |
|---|---|
| IN RE: GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION | MDL Docket No: 2358 |

## RESPONSE OF PLAINTIFF MATTHEW SOBLE IN OPPOSITION TO GOOGLE INC.'S MOTION FOR TRANSFER OF ACTIONS TO THE NORTHERN DISTRICT OF CALIFORNIA AND IN SUPPORT OF TRANSFER TO THE DISTRICT OF DELAWARE

David A. Straite (Del. 5428)
**SIANNI & STRAITE LLP**
1201 N. Orange St., Suite 740
Wilmington, DE 19801
Tel. (302) 573-3560
Fax (302) 358-2975
*dstraite@siannistraite.com*

*Attorneys for Plaintiff Matthew Soble in Soble v. Google Inc., 12-cv-0200-SLR (D. Del.)*

## INTRODUCTION

Matthew Soble, Plaintiff in *Soble v. Google Inc.*, 12-cv-0200-SLR (D. Del.) (hereinafter the "Plaintiff" or "Soble"), submits this Response to Google Inc.'s Motion for Transfer of Actions to the Northern District of California Pursuant to 28 U.S.C. § 1407. Soble concurs that all eight Related Actions identified in the Schedule of Actions accompanying the Motion for Transfer should be consolidated, but opposes transfer to the Northern District of California.

Plaintiff Soble seeks to have all Related Actions transferred and consolidated in the District of Delaware. These actions involve identical factual questions regarding allegations that four companies – California-based Google Inc.; New York-based Vibrant Media Inc.; New York-based Media Innovation Group LLC, and Pennsylvania-based PointRoll Inc. – purposefully circumvented privacy protections in Apple's Safari browser and tracked internet users without their consent in violation of federal and state laws. Soble agrees with Google that transfer and consolidation will further the convenience of the parties and witnesses, and will promote the just and efficient conduct of these cases. However, the District of Delaware, not the Northern District of California, is the appropriate venue for transfer and consolidation because (1) three of the four companies implicated in the scandal are based in the Northeast, not in California, and thus the District of Delaware is far closer to these companies (and indeed, one company, PointRoll, Inc., is based in King of Prussia, PA, just a few miles from the Federal Courthouse in Wilmington, Delaware) and thus the District of Delaware is readily accessible to the bulk of witnesses and documents necessary to prosecute the case; (2) the District of Delaware is the most experienced federal court in the country with complex high technology litigation on a per-judge basis; and (3) the District of Delaware has sufficient resources to handle a case of this complexity.

## FACTUAL BACKGROUND

### I. STANFORD UNIVERISTY RESEARCHER EXPOSES THE SCANDAL

Approximately one month ago, on February 17, 2012, Jonathan Mayer, a researcher at Stanford University, discovered that four companies were surreptitiously circumventing privacy settings on Safari and tracking the internet usage of computer users without authorization. According to Mr. Mayer:

> *Apple's Safari web browser is configured to block third-party cookies by default. We identified four advertising companies that unexpectedly place trackable cookies in Safari. Google and Vibrant Media intentionally circumvent Safari's privacy feature. Media Innovation Group and PointRoll serve scripts that appear to be derived from circumvention example code.*

#### A. California-Based Google

Mr. Mayer observed that with Safari browsers, Google's cookie syncing mechanism involved a special step designed to "trick" the browser into allowing Google's Doubleclick subsidiary to implant tracking cookies. In any browser other than Safari, Google set a "_drt_" social personalization cookie. The cookie was set to expire in 12 or 24 hours, depending on whether the user was logged into Google. However, with Safari, rather than implanting the "_drt_" cookie (which would be blocked by the Safari privacy settings), the server sent back a page that included a form and JavaScript to submit the form to its own URL. The response to the form submission then included the cookie, allowing Google to secretly track users.

### B. New York-based Vibrant Media, New York-based Media Innovation Group, and Pennsylvania-based PointRoll:

Mr. Mayer's investigation determined that three advertising companies in addition to Google were implicated. For example:

1. Vibrant Media

> *Vibrant Media is a contextual advertising network that primarily offers in-text and display advertising. We found conclusive evidence that Vibrant deliberately circumvents Safari's third-party cookie blocking feature: one of the URLs involved in the circumvention is for the resource /safari.jsp.*

2. Media Innovation Group

> *Media Innovation Group (MIG) is an advertising technology provider within the WPP family of companies. MIG's "Zeus Advertising Platform" (ZAP) is WPP's "integrated advertising and analytics platform". According to a report from a vendor, ZAP "is one of the cornerstone products created by MIG" that "provides a holistic view of site analytics and campaign data for a comprehensive understanding of every individual consumer." ZAP "collects and stores over 13 months of historical user-level data and draws from it to provide complex and robust analysis." With ZAP, "MIG is currently tracking the effectiveness of every single advertising element within many live campaigns that reach hundreds of millions of unique users per month . . . ."*
>
> *We found that some MIG advertising content included a script that circumvents Safari's cookie blocking feature . . .*

3. PointRoll

> *PointRoll is a rich media advertising company owned by Gannett. PointRoll's corporate website claims that it "[p]ower[s] 55% of all rich media campaigns online" and "serv[es] over 450 billion impressions for more than two-thirds of the Fortune 500 brands . . . ."*
>
> *We found that a PointRoll cookie helper script circumvents Safari's cookie blocking.*

## II. THE INVESTIGATIONS

After the reports of illicit tracking became public, calls for investigations were immediate. Washington, D.C.-based Consumer Watchdog demanded that the FTC investigate Google, calling its behavior “unfair and deceptive.” It further charged: “Google falsely told Safari users they could control the collection of data by ensuring that third-party cookies were blocked, when in fact Google was circumventing the preference and setting tracking cookies.” Consumer Watchdog also noted that Vibrant Media, Media Innovation Group, and PointRoll were doing the same thing, and “should be closely investigated as well.”

On the same day, the House Bi-Partisan Privacy Caucus wrote to the FTC demanding to know what action the agency was taking to investigate. Similarly, the House Commerce Committee immediately started an investigation of Google, and on February 28, 2012, broadened the investigation to include PointRoll, Vibrant Media and Media Innovation Group. Sen. Jay Rockefeller also weighed in, saying, “According to press reports, Google circumvented consumer choice and may have paved the way for third-party ad networks — including Google's own DoubleClick — to track consumers against their will . . . . If so, this practice may have violated the company's own stated privacy practices. I fully intend to look into this matter and determine the extent to which this practice was used by Google and other third parties to circumvent consumer choice.”

## ARGUMENT

### I. TRANSFER AND CONSOLIDATION OF THE RELATED ACTIONS IS APPROPRIATE BECAUSE THE RELATED ACTIONS INVOLVE COMMON QUESTIONS OF FACT

Multidistrict litigation is governed by 28 U.S.C.A. §1407(a), which provides that when there are civil actions involving one or more common questions of fact pending in different districts, such actions may be transferred to any district for coordinated or consolidated proceedings. "[W]hen two or more complaints assert comparable allegations against identical defendants based upon similar transactions and events, common factual questions are presumed." *In re Air West, Inc. Secs. Litig.*, 384 F. Supp. 609, 611 (J.P.M.L. 1974).

Here, the factual allegations in each of the Related Actions are identical. All relate to the serious allegations of circumventing privacy settings in Apple's Safari browser and tracking internet users without consent. For the reasons set forth in Google's motion, Plaintiff Soble concurs that the Related Actions should be consolidated.

## II. THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE IS THE PROPER FORUM FOR TRANSFER AND CONSOLIDATION

### A. The District of Delaware is a More Convenient Forum for Relevant Witnesses Than The Northern District of California.

Multidistrict litigation is governed by 28 U.S.C.A. §1407(a) which provides that transfers be made by the Judicial Panel on Multidistrict Litigation "upon its determination that transfers for such proceedings will be for the convenience of the parties and witnesses and will promote the just and efficient conduct of such actions." *Id.* Using this statutory instruction, the Panel has repeatedly held that where the defendants are spread throughout the country and no single district has an obvious connection to the case, the Panel will consider a district that is "readily accessible" and "convenient" for the litigants and witnesses. *See, e.g., In re Ins. Brokerage Antitrust Litig.*, 360 F. Supp. 2d 1371, 1373 (J.P.M.L. 2005) ("In concluding that the District of New Jersey is an appropriate forum for this docket, we note that . . . the district offers an accessible metropolitan location that is geographically convenient for many of this docket's litigants and counsel . . ."); *In re Intel Corp. Microprocessors Anti-Trust Litig.*, 403 F. Supp. 2d 1356, 1357 (J.P.M.L. 2005) ("In concluding that the District of Delaware is an appropriate forum for this docket, we observe that . . . the district is an accessible location that is geographically convenient for many of the docket's litigants and counsel . . ."); *see also In re Rembrandt Technologies, LP, Patent Litigation*, 493 F. Supp. 2d 1367, 1370 (J.P.M.L. 2007) (transferring actions to District of Delaware because Delaware was "readily accessible" and convenient for the parties).

Two of the four companies implicated in the "SafariGate" scandal – Google and PointRoll – are already named as defendants in at least one of the Related Actions. Defendant Google is headquartered in Mountain View, California, just a few miles from the Federal Courthouse in San Jose, while Defendant PointRoll is headquartered in King of Prussia, Pennsylvania, just a few miles from the Federal Courthouse in Wilmington, Delaware. It would appear that either District is appropriate; however, the other two companies under investigation – Vibrant Media and Media Innovation Group – are both based in New York, NY, only a two-hour drive from Wilmington, Delaware, but relatively inaccessible to San Jose, California. Employees at these two companies are sure to be witnesses in the MDL, and indeed both companies may soon be defendants in their own right.

If the Panel creates an MDL, witnesses from the four companies will have to travel, and Delaware is more convenient than the Northern District of California for three of the four companies. Witnesses in Pennsylvania and New York will be able to travel by train or car, and not have to fly. When witnesses from Google (the only relevant company based on the west coast) do fly, Wilmington is only 20 minutes from one of the country's largest international airports. And indeed, Google is no stranger to the courts in Delaware: in just 2011 alone, Google was named as a defendant in 29 different actions in the District of Delaware. In another recently-filed action, Google was the plaintiff and chose to sue a Texas-based company in Delaware (not in Texas) despite personal jurisdiction over the defendant in either court. *See Microsoft Corp. and Google Inc. v. GeoTag, Inc.*, 11-cv-0175 (D. Del.).

### B. The District of Delaware is Best Qualified to Manage a Multi-District Litigation Involving Complex Mobile Phone Technology

When choosing a transferee court, one factor the Panel can consider is the relative experience the court or transferee judge has with the type of case at issue. *See, e.g., In re: Flat Glass Antitrust Litig.*, 559 F.Supp.2d 1407, 1408 (J.P.M.L. 2008). No court has more experience with complex high technology cases than the District of Delaware on a per-judge basis.

Because reliable statistics exist for patent infringement cases, they can be a useful proxy when evaluating expertise in "complex high technology" cases such as this one. These statistics paint a picture of clear leadership in the Delaware District Court. For example:

- In 2008, 19 percent of the Delaware District Court's civil docket consisted of patent cases, higher than any other district.
- The Delaware District Court ranks 5th in the country as to overall patent cases filed, even given its small size.
- The Delaware District Court handles more patent cases per year than any other court on a per-judge basis. From 2000-2008, for instance, Delaware District Court judges averaged over thirty patent complaints filed per judge, per year. The next closest jurisdiction came in at a distant second with only fifteen, less than half Delaware's average.

*Source*: Annual Report of the U.S. District Court for the District of Delaware (2009); PriceWaterhouseCoopers, *A Closer Look 2008 Patent Litigation Study: Damages Awards, Success Rate and Time to Trial* (2009).

### C. The District of Delaware Has the Resources to Handle the Complexity of this MDL with the Speed Demanded by the Seriousness of the Allegations

An additional factor that the Panel should consider when selecting a transferee court is whether that court has the resources to handle the litigation. "In concluding that the District of Delaware is an appropriate forum for this docket, we observe that . . . the district is well equipped with the resources that this complex anti-trust docket is likely to require. . . ." *In re Intel Corp. Microprocessors Anti-Trust Litig.,* 403 F.Supp.2d 1356, 1357 (J.P.M.L. 2005). According to statistics provided by the Panel, as of March 12, 2012, there were only two MDLs pending in the District of Delaware, down from five as recently as September 30, 2011. Contrast this with 22 in the Northern District of California, the heaviest burden in the country other than the Southern District of New York. Indeed, even on a per-judge basis, the burden is only half as great in Delaware, because Delaware's two MDLs are spread among four available Article III judges, whereas the Northern District of California's 22 cases are spread among 20 Article III judges. Finally, it should be noted that just last year, Judge Andrews of the District of Delaware took his oath of office, eliminating the final vacancy in the court. Having a full complement of judges provides important resources for an MDL of this magnitude.

## **CONCLUSION**

Transfer of the Related Actions to a single judge in the District of Delaware pursuant to 28 U.S.C. § 1407 is appropriate. The Related Actions involve common questions of fact – each contains similar allegations of the knowing circumvention of Safari's privacy settings. Transfer to a single judge in Delaware will also serve the convenience of the parties and the witnesses because it is the most readily accessible venue to the largest number of witnesses and Defendants. No other federal court has as much experience with complex high technology cases on a per-judge basis as the District of Delaware, and has sufficient resources to manage this proposed MDL.

Respectfully submitted,

Dated: March 22, 2012

**Sianni & Straite LLP**

*/s/ David A. Straite*
David A. Straite (Del. 5428)
1201 N. Orange St., Suite 740
Wilmington, DE 19801
Tel. (302) 573-3560
Fax (302) 358-2975
*dstraite@siannistraite.com*

*Attorneys for Plaintiff Matthew Soble in Soble v. Google Inc., 12-cv-0200-SLR (D. Del.)*

**BEFORE THE UNITED STATES JUDICIAL PANEL ON MULTIDISTRICT LITIGATION**

| | |
|---|---|
| IN RE: GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION | MDL Docket No: 2358 |

## CERTIFICATE OF SERVICE

I, David A. Straite, counsel for Matthew Soble, Plaintiff in *Soble v. Google Inc.*, 12-cv-0200-SLR (D. Del.) certify that on March 22, 2012, I served the following document on counsel of record in MDL 2358 via the Court's ECF system:

1. RESPONSE OF PLAINTIFF MATTHEW SOBLE IN OPPOSITION TO GOOGLE INC.'S MOTION FOR TRANSFER OF ACTIONS TO THE NORTHERN DISTRICT OF CALIFORNIA AND IN SUPPORT OF TRANSFER TO THE DISTRICT OF DELAWARE

Dated: March 22, 2012

*/s/ David A. Straite*
**Sianni & Straite LLP**
David A. Straite (Del. 5428)
1201 N. Orange St., Suite 740
Wilmington, DE 19801
Tel. (302) 573-3560
Fax (302) 358-2975
*dstraite@siannistraite.com*

*Attorneys for Plaintiff Matthew Soble in Soble v. Google Inc., 12-cv-0200-SLR (D. Del.)*